UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Valter Delgiusto

Varovanje omrežij pred sodobnimi grožnjami s požarnimi zidovi naslednje generacije

DIPLOMSKO DELO NA UNIVERZITETNEM ŠTUDIJU

Mentorica: doc. dr. Mojca Ciglarič

Ljubljana, 2016

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisani, Valter Delgiusto, z vpisno številko 63020028, sem avtor diplomskega dela, z naslovom:

Varovanje omrežij pred sodobnimi grožnjami s požarnimi zidovi naslednje generacije.

S svojim podpisom zagotavljam da:

- sem diplomsko delo izdelal samostojno, pod mentorstvom doc. dr. Mojce Ciglarič,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela, v zbirki »Dela FRI«.

Zahvala

Iskreno se zahvaljujem mentorici, doc. dr. Mojci Ciglarič, za strokovno usmerjanje in usmerjanje pri nastanku tega diplomskega dela.

Zahvaljujem se podjetjema Projekt IP d.o.o. in S&T Slovenija d.d., za izposojo opreme in prostorov ter Marku Ostanku za nasvete in pomoč pri praktični izvedbi diplomskega dela.

Hvala družini in ostalim, ki so me med študijem in v času nastajanja diplomskega dela podpirali.

Kazalo

Povzetek

Ker klasični požarni zidovi že dolgo niso kos modernim grožnjam, ki prežijo na vsakodnevne uporabnike interneta, smo v diplomskem delu želeli preučiti njihove naslednike – požarne zidove naslednje generacije.

V prvem delu diplomskega dela opisujemo moderne grožnje in napade. Podrobno smo opisali DoS in APT napada, ki sta med njimi najbolj pogosta in katera lahko povzročita največ škode v sistemu, ki ga napadeta. Nato smo podali teoretične osnove delovanja požarnih zidov ter opisali funkcionalnosti požarnih zidov naslednje generacije.

V nadaljevanju smo izvedli različne teste na treh požarnih zidovih naslednje generacije, analizirali rezultate testov ter jih predstavili. Cilj diplomskega dela je bil ugotoviti, ali lahko požarni zidovi naslednje generacije ustrezno nadomestijo klasične požarne zidove in tako pripomorejo k ustrezni zaščiti uporabnikov interneta.

Ključne besede:
Požarni zid naslednje generacije, varnost, DoS napad, APT napad.

Abstract

Classic firewalls have long been unable to cope with modern threats that ordinary Internet users are exposed to. This thesis discusses their successors - the next-generation firewalls.

The first part of the thesis describes modern threats and attacks. We described in detail the DoS and APT attacks, which are among the most frequent and which may cause most damage to the system under attack. Then we explained the theoretical basics of firewalls and described the functionalities of next generation firewalls.

In the following chapter we performed various tests on three models of next-generation firewalls analyzing and presenting the test results. The aim of the thesis was to determine whether the next-generation firewalls are appropriate to replace conventional firewalls and so to contribute to the adequate protection of Internet users.

Key words:

Next- generation firewall, security, DoS attack, APT attack.

1. Uvod

Uporaba internetnega omrežja se povečuje vsakodnevno in s tem se povečuje tudi število uporabnikov. Globalno omrežje je postalo nepogrešljiv pripomoček, tako pri opravljanju delovnih obveznosti, kot tudi v prostem času in je praktično spremenil način našega življenja.
Pri uporabi interneta pa na uporabnike ter organizacije, v katerih uporabniki delujejo, prežijo številne grožnje. Napadalci skušajo z uporabo zlonamerne programske opreme uporabniku onemogočiti uporabo interneta, uničiti ali protipravno pridobiti kritične informacije, intelektualno lastnino ipd., z namenom pridobivanja finančne koristi ali konkurenčne prednosti. Zato morajo organizacije poskrbeti za ustrezno zaščito pred omenjenimi napadi.

Pred nastopom globalizacije in prave »eksplozije« interneta, so bila omrežja organizacij toga. Obstajala je natančno določena meja med notranjim omrežjem organizacije in internetom. Večina aplikacij in za poslovanje pomembnih resursov se je nahajala znotraj omrežja organizacije. Na robu med internim varovanim omrežjem in internetom, se je nahajal požarni zid, ki je skrbel za varnost naprav, ki so se povezovale v internet. Promet proti internetu in iz interneta proti omrežju je bil predvidljiv, aplikacije so bile jasno definirane. Tako je lahko požarni zid, s statičnimi varnostnimi pravili, korektno opravljal svojo nalogo in ščitil omrežje organizacije pred zunanjimi vplivi.
Stanje se je v zadnjih nekaj letih drastično spremenilo. Zaradi globalizacije, veliko dostopnejših možnosti povezovanja, mobilnosti, virtualizacije in pojava računalništva v oblaku, so se realnosti omrežnega povezovanja popolnoma spremenile. Hitra evolucija interneta in aplikacij je prinesla s seboj čisto drugačen način komunikacije uporabnikov v internet. Seveda so se vzporedno širile in razvijale tudi grožnje, ki prežijo na uporabnike, katerim pa standardni požarni zidovi niso več kos in pojavila se je potreba po naprednejši zaščiti sistemov.
Strokovnjaki za omrežno varnost so razvili *»Next Generation Firewall«* oziroma požarni zid naslednje generacije, ki temelji na inovativnem pristopu pri analizi omrežnega prometa in zagotavljanju varnosti. Ker so požarni zidovi naslednje generacije razmeroma nov produkt na tržišču, še ne obstajajo standardi, katere morajo izpolnjevati. Tudi cena takšnih požarnih zidov je višja, v primerjavi s tradicionalnimi.

Ker tradicionalni požarni zidovi niso več dovolj za zagotavljanje varnosti organizacije, smo se odločili, da bomo opravili analizo zmogljivosti in učinkovitosti požarnih zidov naslednje generacije in tako pomagali organizacijam pri odločitvi, ali je takšen požarni zid prava izbira za izboljšanje njihove omrežne varnosti.
V nadaljevanju bomo podali pregled sodobnih omrežnih grožen in napadov ter navedli nekaj informacij omrežnih grožnjah, sami tehnologiji omrežij, omrežni varnosti in požarnih zidovih.

V diplomskem delu smo izvedli praktične teste na treh požarnih zidovih naslednje generacije z namenom:

- analizirati zmogljivosti požarnih zidov in tako preveriti ali izpolnjujejo današnje zahteve po visokih hitrostih povezovanja v internet,
- analizirati učinkovitost požarnih zidov naslednje generacije pri zaščiti omrežja pred najpogostejšimi modernimi grožnjami, kot so DoS napadi ter APT napadi,
- podati oceno, ali so požarni zidovi naslednje generacije primerna in zadostna zaščita sodobnih omrežij organizacij.

V sklepnem delu smo preučili rezultate testov, jih pokomentirali ter podali oceno, ali lahko požarni zid naslednje generacije dejansko pripomore k izboljšanju informacijske varnosti.

2. Sodobne omrežne grožnje in napadi

Z večanjem števila uporabnikov povezanih v svetovni splet se veča tudi število groženj, ki prežijo na posameznega uporabnika oz. organizacije. IT strokovnjaki ugotavljajo, da večina kibernetskih groženj preide v omrežje organizacije iz interneta.

Pred leti so bile največje grožnje za uporabnike interneta naslednje:

- virusi in črvi,
- trojanski konji,
- SPAM oz. nezaželena elektronska pošta,
- phishing oz. ribarjenje,
- packet Sniffing oz. vohljanje,
- spletne strani z zlonamerno programsko kodo,
- napadi na gesla.

Z napredovanjem informacijske tehnologije in bliskovitim večanjem števila naprav in uporabnikov povezanih v internet, so se tudi grožnje razvile in spremenile. Kibernetični kriminal je postal sredstvo za pridobivanje finančne koristi in razvil se je pravi sistem za podporo kibernetičnim kriminalcem. Le ti lahko danes z lahkoto pridejo do različnih orodij za ustvarjanje groženj in napadov – kupijo jih na črnem trgu. Specializacija in lahka dostopnost do takšnih orodij je privedla do neverjetnega porasta groženj in kibernetičnega kriminala [1].

Tako lahko danes zasledimo predvsem naslednje internetne grožnje [2]:

- DoS (ang. Denial of Service) napade oz. napade za zavrnitev storitve,
- APT (ang. Advanced persistenet Threat) oz. napredne trajne grožnje,
- Zero-day napade,
- Ransomware oz. izsiljevalske viruse,
- Watering Hole napade,
- krajo identitete,
- napade na mobilne naprave,
- Phishing napade in napade s socialnim inženiringom.

V nadaljevanju bomo prvi dve grožnji iz seznama, ki sta danes tudi najbolj pogosti, podrobneje opisali.

2.1 DoS napadi

DoS (ang. Denial of Service) napad ali napad za zavrnitev storitev je vrsta napada, kjer napadalci skušajo onemogočiti legitimnim uporabnikom dostop do določenih storitev. Čeprav se načini, motivi in cilji DoS napada lahko razlikujejo, je običajno napad prizadevanje ene ali več oseb, da bi trajno ali začasno onemogočila učinkovito delovanje internet strani ali storitve. Cilji izvajalcev DoS napada so običajno lokacije in storitve spletnih ponudnikov, kot so banke in DNS strežniki. Ena od običajnih metod napada vključuje zasičenje cilje naprave z zunanjimi komunikacijskimi zahtevki na način, da naprava ne more odgovoriti ali odgovarja tako počasi, da postane nedosegljiva. DoS napad je implementiran tako, da prisili računalnik naj izkoristi vse svoje resurse in tako ne zmore nuditi uslug legitimnim uporabnikom.
Izvajanje DoS napada se smatra kot kršenje »Internet Proper Use Policy« pravila, kot tudi kršitev zakonodaje posameznih držav.

Osnovne značilnosti DoS napadov:
United States Computer Emergency Readiness Team definira simptome DoS napada kot:

- nenavadna počasnost omrežja (pri odpiranju datotek ali dostopu do spletne strani),
- nerazpoložljivost določenih spletnih strani,
- nezmožnost dostopa do katerekoli spletne strani,
- drastično povečanje števila prejetih "spam" sporočil elektronske pošte (ta vrsta DoS napada se imenuje "Mail-bomba") [3].

Za DoS napad je značilno izrecen poizkus napadalca, da prepreči legitimnim uporabnikom uslug koriščenje le teh. Napadi so lahko usmerjeni na katero koli mrežno napravo, vključno z usmerjevalniki, strežniki elektronske pošte in DNS strežniki [4].

2.1.1 Osnovna delitev DoS napadov

DoS napade lahko delimo v dve skupini. Pri vseh DoS napadih gre za napad na ciljni sistem, s pošiljanjem paketov, razlikujejo pa se v vrsti sporočila oz. paketa, ki ga pošljejo žrtvi.

Napadi, ki izkoriščajo ranljivosti sistemov
Sporočila so poslana specifični aplikaciji ali delu sistemske programske opreme, ki vsebuje ranljivost. Ta posebno oblikovana sporočila izkoriščajo ranljivosti in privedejo sistem v stanje nezmožnosti obdelovanja zahtev. V tem primeru govorimo o aplikacijskem DoS napadu, oziroma je tehnični izraz za tak napad "izkoriščanje ranljivosti" (ang. Vulnerability attack) [4].

»Flooding« napadi ali napadi s poplavljanjem

Pri tem napadu gre za pošiljanje velikega števila legitimnih sporočil ciljnemu sistemu, z namenom uporabe celotnega komunikacijskega kanala ali se zasedbe ključnih resursov sistema (pomnilnik, procesor, itd.). Sistem se tako preobremeni in prepreči se mu pravilno delovanje. Da bi to lahko dosegel, mora imeti napadalec naprave, ki so sposobne ustvariti veliko več sporočil, kot jih napadli strežnik lahko obdela v omejenem času. Seveda so komercialni spletni strežniki grajeni s ciljem obdelave velike količine prometa, tako da jih napadalci težko prizadenejo, če napadajo samo iz ene strani. V tem primeru napadalci uporabijo računalnike, na katerih so pridobili nadzor izkoriščanjem ranljivosti in krajo administratorskih pravic, običajno s pomočjo *Rootkit* orodij. Z zbirnim napadom iz vseh računalnikov, nad katerimi so pridobili nadzor (ang. Botnet), napadejo sistem z več strani in tako povzročijo zasedbo resursov [4].

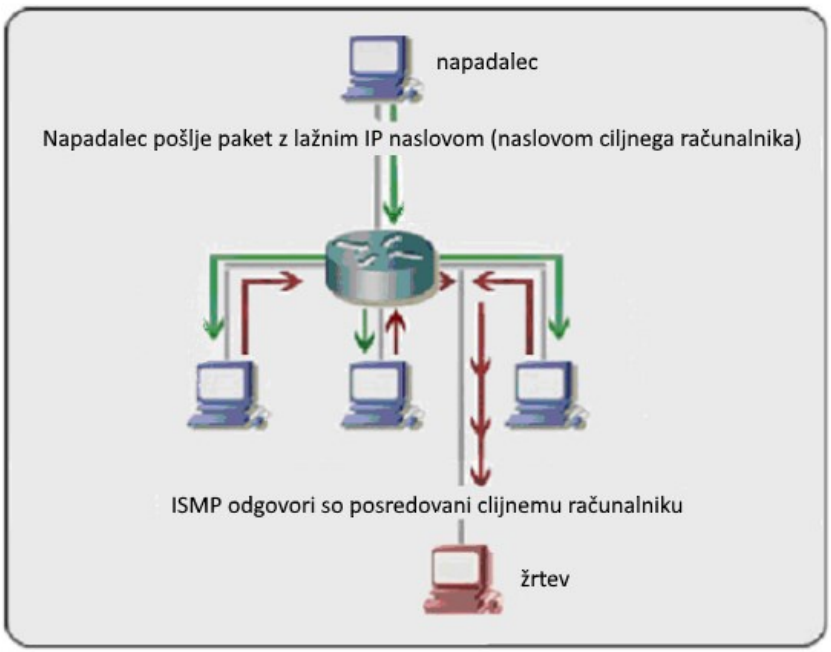
2.1.2 Vrste DoS napadov

»ICMP flood« napadi

V to kategorijo spadajo vsi napadi, ki temeljijo na ICMP (ang. Internet Control Message Protocol) protokolu, ki je eden izmed temeljnih protokolov znotraj TCP/IP skupine protokolov. Protokol primarno služi za pošiljanje kontrolnih sporočil znotraj omrežja, za razliko od npr. UDP ali TCP protokolov, kateri služijo za prenos podatkov. Napadi zlorabljajo način, kako protokol odgovarja na kontrolne signale za preplavljanje omrežja žrtve. Med te napade uvrščamo: smurf, ping flood, ping of death, SYN napade, Nuke in TearDrop napade. Obstajajo še drugi, vendar so manj pogosti [4].

»Smurf« napad

»Smurf« napad je posebna inačica flood DoS napadov. Izkorišča slabo konfigurirane omrežne naprave, katere omogočajo pošiljanje paketov na vse uporabnike določenega omrežja, preko naslova za razpošiljanje (ang. broadcast). Omrežje v tem primeru služi kot »smurf« ojačevalec. Pri tem napadu izvršitelji pošiljajo usmerjevalniku velike količine »echo« zahtevkov, kjer je izvorni IP naslovi zamenjan z IP naslovom žrtve, najpogosteje je to kar usmerjevalnik sam. Usmerjevalnik nato posreduje zahtevke na celotno podomrežje, vse naprave v omrežju na ta zahtevke odgovorijo in tako hitro zapolnijo komunikacijske kapacitete, kar onemogoča, da bi legitimni paketi dosegli svoj cilj. Danes takšni napadi uspevajo redko, ker je zaščita pred takšnimi napadi enostavna in je v bistvu postala standardna lastnost usmerjevalnikov – onemogočanje pošiljanja na broadcast naslove [4].



Slika 1: Scenarij »smurf« napada [4].

»PING flood« napad

PING poplavljanje temelji na pošiljanju veliko »ping« paketov, običajno z uporabo »ping -f« ukaza. Zagon je zelo preprost, napad pa temelji na predpostavki, da ima napadalec na razpolago večjo pasovno širino kot žrtev. Uspešnost napada je večja, če žrtev odgovarja z echo reply paketi [4].

»PING of death« napad

Kljub zastrašujočemu nazivu je to enostaven tip DoS napada, kjer se izkorišča napaka v implementaciji TCP/IP protokola. Temeljni na nesposobnosti obdelave ping paketa, večjega od največje dovoljene velikosti paketa znotraj IPv4 definicije. Takšni napadi so bili mogoči na večino naprav vključno z Linux, Unix, Mac, Windows, printerji in router napravami. Danes ima samo še zgodovinski pomen, saj so bile napake v implementaciji že davno sanirane [4].

»Teardrop« napad

»Teardrop« napad vključuje pošiljanje poškodovanih IP fragmentov, s prekrivanjem (ang. overlapping) na ciljni računalnik. Ranljivost v kodi za TCP / IP fragmentacijo številnih operacijskih sistemov povzroči nepravilno rokovanje s fragmenti ter padec sistema kot rezultat. IP (ang. Internet Protocol) paket, ki je prevelik za usmerjanje, se deli na fragmente, v katere se vpisuje oddaljenost od začetka paketa, kar omogoča ponovno sestavljanje paketa na strani prejemnika. Pri tem napadu napadalec vnese lažno razdaljo v enega izmed fragmentov. Če

prejemnik paketa nima ustreznega mehanizma za tak slučaj, lahko sistem pade. Takšnim napadom so podvrženi predvsem starejši operacijski sistemi [4].

»Nuke« napad

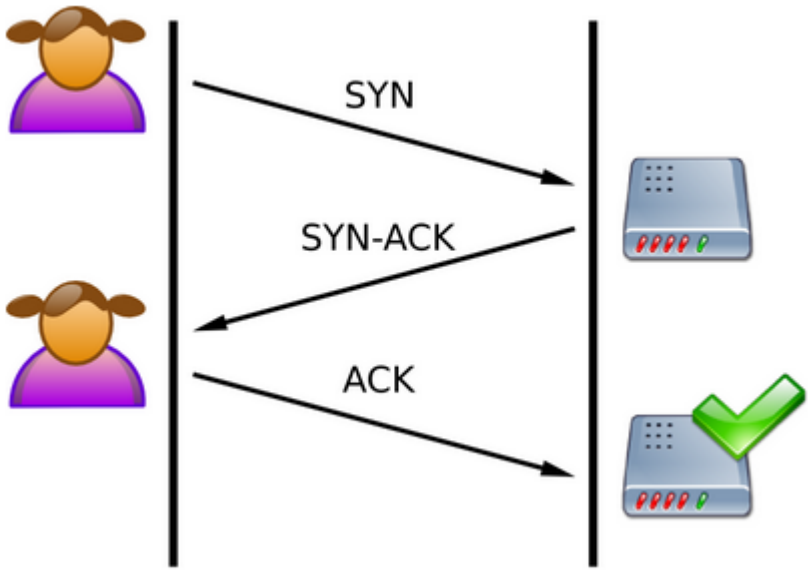
»Nuke« je starejši tip DoS napada na računalniška omrežja, kateri temelji na pošiljanju fragmentiranih in poškodovanih ICMP paketov na cilj. To dosežemo z uporabo modificiranega PING orodja za večkratno pošiljanje takih paketov, s čimer se upočasni delovanje ciljnega računalnika, vse dokler ne pride do popolne prekinitve [4].

»SYN flood« napad

Vrsta DoS napada, pri katerem napadalec pošlje niz TCP / SYN (ang. synchronize) zahtev žrtvi. Prekinitev storitve dosežemo z izkoriščanjem TCP protokola in načina, kako vzpostavlja povezavo med napravama. Odjemalec in strežnik si izmenjata niz sporočil na sledeči način:

1. Odjemalec zahteva vzpostavitev povezave z pošiljanjem SYN sporočila strežniku.
2. Strežnik odgovori in potrdi vzpostavitev povezave z pošiljanjem SYN-ACK (synchronize-acknowledge) sporočila odjemalcu.
3. Odjemalec potrdi z pošiljanjem ACK sporočila in s tem je povezava vzpostavljena.

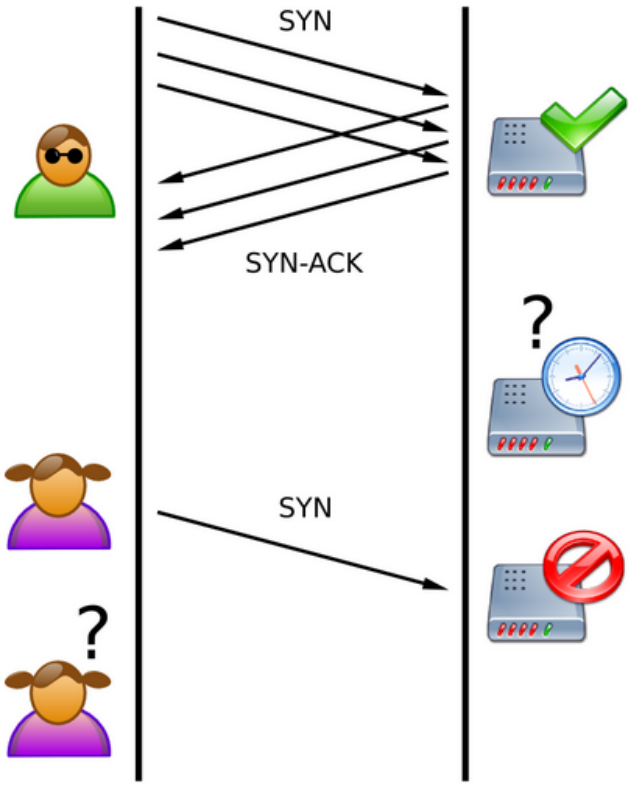
Postopek je tudi prikazan na spodnji sliki:



Slika 2: Prikaz vzpostavitve TCP povezave [4].

Tovrstna vzpostavitev komunikacije se imenuje tudi TCP trojno rokovanje, kjer je legitimni uporabnik prikazan na sliki levo, desno pa strežnik, na katerega pošlje zahtevo za povezavo.

Ranljivost temelji na dolžnosti strežnika, da registrira vse SYN zahtevke in jih hrani v pomnilniku, dokler se povezava ne vzpostavi. Napadalec izkorišča ta princip delovanja tako, da pošlje več SYN zahtev, z lažnimi izvornimi IP naslovi ali iz drugih računalnikov. Tako dobi odgovor v obliki SYN-ACK sporočila, vendar nikoli ne odgovori na zahtevo z ACK sporočilom. Tako prisili strežnik, da ohranja pol-odprte povezave v spominu. Ko izkoristiti vse vire za hrambo pol odprtih povezav, strežnik ne more več obdelati novih legitimnih SYN zahtev in s tem zavrne storitev rednim strankam. Napad se dejansko lahko izvede tako, da napadalec spremeni izvorni IP naslov ali uporabi odjemalca, ki ne oddaja ACK sporočil. Primer je podan na spodnji sliki xx, kjer je napadalec prikazano z zeleno [4].



Slika 3: Prikaz SYN flood napada [4].

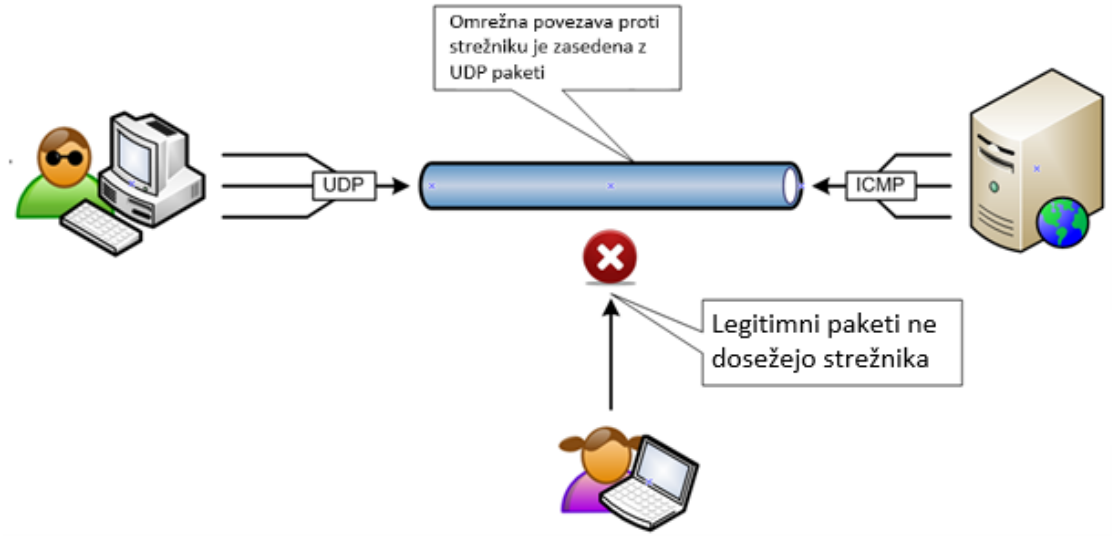
»UDP flood« napad

Napad s pomočjo UDP protokola se močno razlikuje od napadov preko TCP protokola. Glede na to, da UDP ne zagotavlja dostave sporočila in ne pričakuje potrditev vzpostavitve povezave s pošiljanjem potrditvenih sporočil (SYN, SYN-ACK, ACK), ta napad temelji na pošiljanju velikega števila UDP paketov na naključno izbrana vrata (eng. Port) računalniškega sistema. Po prejemu paketa strežnik:

- preveri katera storitev posluša na izbranih vratih,
- spoznal da take aplikacije ni ter

- odgovori na zahtevo z ICMP Destination Unreachable paketom (cilj je nedosegljiv).

S takšnim načinom obdelave paketov bo strežnik sam sebi zasedel celotno povezavo, z odgovarjanjem na veliko število lažnih UDP paketov. Ta scenarij je prikazana na spodnji sliki [4].



Slika 4: Prikaz UDP flood napada [4].

DDoS napad

Do porazdeljenega napada za prekinitve storitev (ang. Distributed Denial of Service) pride, ko se več predhodno okuženih sistemov poveže v t.i. »botnet« in poplavijo oz. zasedejo resurse ciljnih sistemov. Običajno je to en ali več spletnih strežnikov. DoS napadi temeljijo na veliki količini podatkov, s katerimi je žrtev preplavljena, najpogosteje pa se izvajajo kot DDoS napadi. Poudarek pri teh napadih je, da več sistemov nadvlada enega. Delimo jih v dve osnovni skupini:

- neposredni DDoS napadi,
- posredni DDoS napadi.

Priprava za DDoS napad

Za svojo izvedbo DDoS napadi zahtevajo veliko število računalnikov, ki so pripravljeni izvesti napad sinhrono, ob ukazu napadalca. Tak računalniški sistem ni zgrajen čez noč in obstaja veliko tehnik, ki jih vešči kriminalci uporabljajo za okupacijo sistemov ostalih uporabnikov. Med njimi se najpogosteje uporabljajo trojanski konji in virusi, ki se propagirajo od sistema do sistema ter aplikacije z znanimi ranljivostmi, ki jih napadalci uporabljajo za pridobitev skrbniške pravice nad sistemom. Z dodajanjem novih računalnikov se povečuje velikost

botneta, hkrati pa napadalci uporabljajo na novo okužene računalnike, da še naprej napadajo in pridobivajo nove nezaščitene sisteme. S povečanjem in strukturiranjem botneta, napadalec povečuje svojo sposobnost napadanja. Iskanje ranljivih računalnikov poteka na več načinov:

Naključno skeniranje (ang. Random Scanning) − naprava, na kateri deluje zlonamerna programska oprema, poljubno izbere IP-naslov iz določenih IP naslovnega prostora in išče ranljivosti. Ko jih najde, požene na ciljnem sistemu enako zlonamerno programsko opremo, kot teče na njem. Prednost te tehnike je možnost hitrega širjenja zlonamerne kode in ustvarjanje majhne količine prometa (tako je tehniko težje odkriti).

Skeniranje iz seznama zadetkov (ang. Hit-List scanning) − pred začetkom skeniranja napadalec pripravi seznam velikega števila potencialno ranljivih računalnikov. Skeniranje se izvaja po seznamu, ko napadalec najde ranljiv računalnik, na njem zažene zlonamerno kodo. Takrat se seznam razdeli na dva dela ter pol seznama prejme na novo okužen računalnik. Prednost te metode je v tem, da se v zelo kratkem času zažene zlonamerna koda na vseh ranljivih napravah na seznamu, saj se seznam razdeli in zmanjša vsakič, ko najde novo ranljivo napravo.

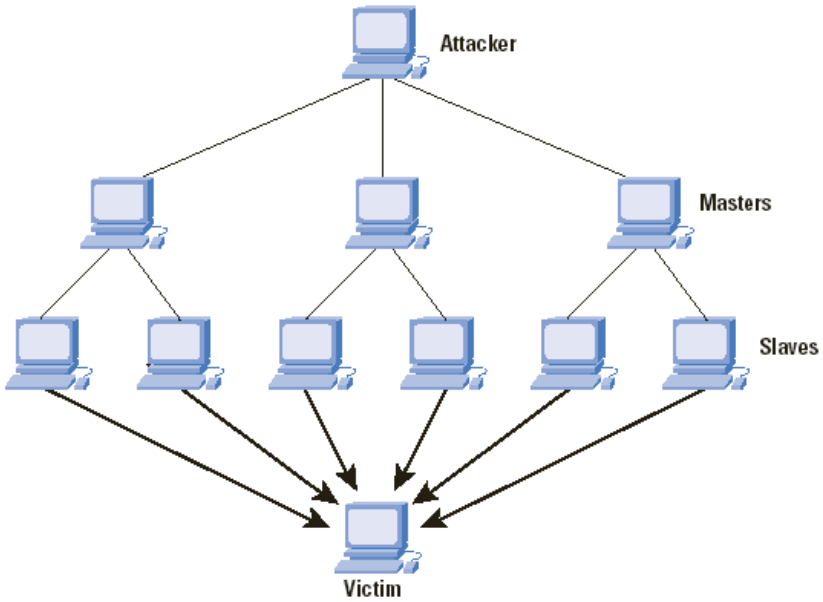
Topološko skeniranje (ang. Topological scanning) − ta metoda uporablja informacije (URL podatke), shranjene na izpostavljenem ranljivem računalniku, da bi našla nove cilje. Prednost te metode je visoka natančnost in hitro ustvarjanje vojske računalnikov.

Skeniranje lokalnega podomrežja (ang. Local subnet scanning) − ta vrsta skeniranje deluje na področju za požarnim zidom, torej v območju za katerega se smatra, da je zaščiten pred skeniranjem. Strežnik išče ranljive računalnike v lokalnem omrežju. Prednosti te metode so, da jo je mogoče uporabiti v kombinaciji z drugimi metodami in tako doseči hitro širjenje.

Skeniranje s permutacijami (ang. Permutation scanning) − vsi računalniki si delijo skupen seznam IP naslovov. Po odkritju in zasedbi novega ranljivega računalnika, le ta začne s skeniranjem iz poljubnega mesta v seznamu. Metoda se lahko uporablja v kombinaciji z ostalimi metodami ter se tako doseže hitro širjenje mreže okuženih računalnikov [4].

Izvedba DDoS napada

Ko je botnet mreža dovolj razširjena, se strukturira na način, da napadalec komunicira le z majhnim številom računalnikov, imenovanih gospodarji, (ang. bot herder, master), ki nadzirajo napadalne sisteme (ang. Bot, Zombie). Tako je napadalca težje izslediti preko IP naslova (ang. Back-tracking). Sledi primer DDoS napada.

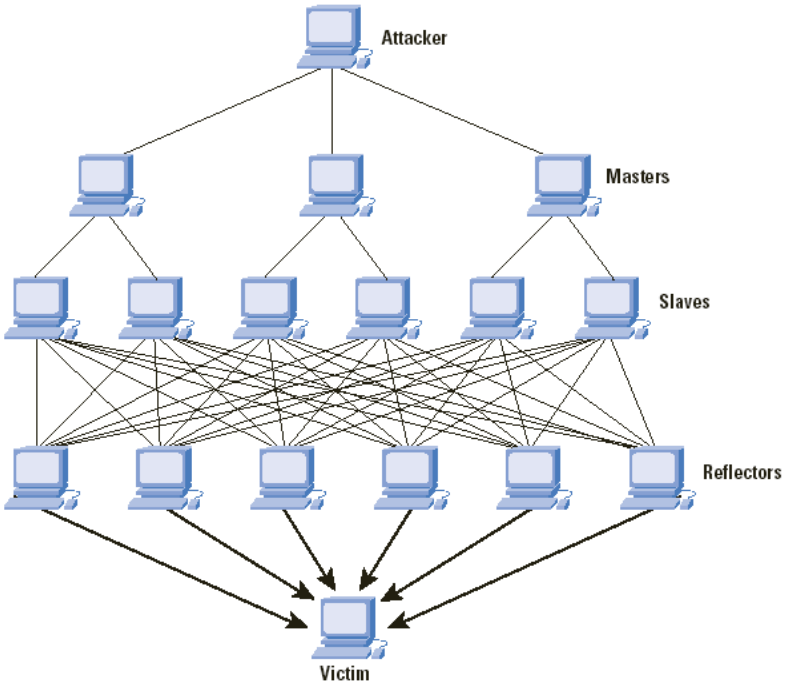


Slika 5: Izvedba DDoS napada [4].

Tako strukturiran sistem je pripravljen za napad ob ukazu napadalca. Po poslanem ukazu gospodarjem, le ti posredujejo IP naslov cilja bot napravam in napad se prične. Pogosto napadalci dajejo v najem svoje botnet mreže. V primeru, da napadalec nima lastne botnet mreže, jo najame ter preko te izvede napad [4].

DRDoS napad

Kratico DRDoS uporabljamo za »Distributed reflected denial of service attack« napad. Ta napad uporablja računalnike izven botnet mreže, ki jim pravimo »reflektorji«, ter jim posreduje zahteve, ki jih odbijejo proti ciljnemu sistemu napada. Napad je izveden tako, da botnet mreža pošlje veliko količino ICMP zahtev z lažnim izvornim IP naslovom, ki je zamenjan z naslovom žrtve. Tako se te zahteve »odbijejo« od reflektorjev do ciljnega sistema. S takšno obliko napada se število zahtev večkratno poveča in s tem se veča tudi učinkovitost napada. Spodnja slika prikazuje scenarij takšnega napada [5].



Slika 6: prikaz DRDoS napada [4].

»Peer-to-peer« napadi

Specifičnost te vrste DDoS napada je, da ne koristi botnet mreže računalnikov za zagon, ampak uporablja legitimne uporabnike omrežij peer-to-peer. Z uporaba številnih peer-to-peer omrežij (povezava ena na ena) napadalci izkoriščajo ranljivosti v teh, za začetek DDoS napadov, na sistem žrtve. Pri izvedbi napada, napadalec uporabnikom peer-to-peer omrežja vpiše sistem žrtve kot izvor deljene datoteke. Tako se tisoče uporabnikov agresivno povezuje na ciljno napravo, z namenom prenosa željene datoteke. Tipični spletni strežnik lahko obdela več sto povezav na sekundo, preden mu začnejo zmogljivosti upadati, čeprav je večina spletnih strežnikov sposobna obdelati tudi do pet ali šest tisoč zahtev na sekundo. Med peer-to-peer napadi je lahko srednje velika spletna stran napadena s približno 800.000 zahtevami v kratkem času. Čeprav je te vrste napad mogoče enostavno prepoznati s pomočjo edinstvenih podpisov kode paketov (ang. Signatures), takega nenadnega števila povezav ni mogoče filtrirati [4].

Razlika med DoS in DDoS napadi

Razlika med tema dvema vrstama napadov je očitna. Na splošno lahko opredelimo, da vsak napad, ki vključuje več napadalcev, ki poskušajo doseči zavrnitev storitve, imenujemo DDoS napad. V nasprotnem primeru gre za DoS napad. Čeprav se struktura napadov razlikuje od napada do napada, je večina DoS napada izvedena kot DDoS napad, predvsem zaradi višje učinkovitosti le tega.

2.2 Primer DoS napada

Pri napadu na strežnike podjetja CloudFlare leta 2014 so napadalci izkoristili ključno ranljivost v infrastrukturi interneta in izvedli, po opisu varnostnih raziskovalcev, največji svetovni Denial of Service (DoS) napad do takrat.
Resnost DoS napada se meri v količini zasedene pasovne v gigabitih na sekundo (Gbs). Ta napad je dosegel 400Gbps - več kot 100Gbps več kot v predhodnem največjem napadu. Tarča tega destruktivnega prometa so bili strežniki podjetja »CloudFlare«, ki je specializirano za zaščito ravno pred takšnimi napadi. Strežniki iz vseh podatkovnih centrov podjetja so bili dalj časa nedosegljivi, napad pa je povzročil omrežne zastoje v delu evropskega internet omrežja.
Matthew Prince, izvršni direktor CloudFlare, je napad komentiral na Twitterju: "Nekdo je pridobil nov, velik top. To je šele začetek slabega, ki še pride."
Napad je bil izjemen, ne samo zaradi svoje velikosti, ampak tudi zaradi načina kako je izkoristil vrsto strežnika, ki se uporablja za sinhronizacijo časa na internetu – Network Time Protocol (NTP) strežnika.
Na tisoče takšnih strežnikov je porazdeljenih po vsem svetu, z namenom ohranjanja naprav v časovni sinhronizaciji. Če se čas med sistemi ne sklada, lahko hitro nastopijo težave: E-pošta lahko prispe še preden je bila poslana, računalnik lahko prejme navodila za dogodke iz preteklosti.
CloudFlare je v objavi pojasnil metodo napada, kjer je podal primer NTP strežnika podjetja Apple, ki se imenuje "time.euro.apple.com". Mac naprave v tem časovnem pasu pošiljajo zahteve na strežnik, da se prepričajo ali je njihova ura sinhronizirana. NTP strežniki pa uporabljajo Univerzalni koordinirani čas (UTC).
Obstajata dve ranljivosti v takem sistemu. Prvič, podatki, ki jih NTP strežnik pošlje kot odgovor, so veliko večji od prvotne zahteve, in drugič, te zahteve so lahko tarča »spoofing« prevar, kar pomeni, da lahko hekerji ukanejo strežnik, naj informacijo vrne na drugi IP naslov, ne pa na izvornega. Z združevanjem teh dveh lastnosti se lahko NTP strežniki uporabi predvsem kot ojačevalec za napade. Napadalci so poslali veliko količino zahtevkov za podatek o točnem času in preusmerili odgovor strežnika na nič hudega sluteč sistem in ga preplavili z mrežnim prometom.
Pošiljanje podatkov o času morda ne zveni kot podatkovno intenzivno, zato je CloudFlare izvedel preprost test, v katerem je dosegel "faktor ojačitve" 206x. To pomeni, da lahko z uporabo te metode, napadalec s pasovno širino povezave 1Gbps ustvari 206 Gbps prometa proti ciljnemu sistemu.
Skrbniki spletnih storitev lahko s preprostimi nadgradnjami omilijo takšne vrste napadov, vendar so strokovnjaki v tehnoloških skupnostih zaskrbljeni, da bodo tudi v prihodnje ponudniki internet storitev prepočasni ali nevešči pri zaščiti njihovih spletnih storitev [6,7].

2.3 APT napadi

APT (Advanced Persistent Threat) ali napredne trajne grožnje opredeljuje kategorijo usmerjenih napadov oblikovanih posebej za ciljnega posameznika ali organizacijo, z namenom pridobivanja kritičnih informacij. Napredne trajne grožnje so zasnovane na način, da ostanejo skrite v sistemu, kar se da dolgo. V sistemu se premikajo počasi in brez puščanja sledi z namenom, da se izognejo zaznavi in odkritju. Za razliko od tradicionalnih napadov, ki so hitro izvedeni in imajo za cilj hitro pridobivanje koristi (predvsem finančnih), lahko imajo APT-ji cilj mednarodnega, industrijskega ali konkurenčnega vohunstva in / ali sabotaže. Cilj večine APT napadov je pridobivanje informacij iz sistema »napadene« organizacije (npr. poslovne skrivnosti, intelektualno lastnino, »know-how«, tehnološke in proizvodne podatke ipd.).
APT-ji se namreč razlikujejo od ostalih tradicionalnih groženj in napadov zaradi sledečih lastnosti: ponavljajočega opravljanje ciljev, prilagajanja in vztrajnosti.
Značilnost APT je tudi ta, da predstavlja dolgoročen napad, ki ne sledi hitremu doseganju ciljev, značilnim za večino napadov, izvedenih z zlonamerno programsko opremo. Tako je cilj APT, da ostane kar se da dolgo neodkrit ter da v tem obdobju izvaja in uporablja različne vrste napadov. APT izvajalcu napada omogoča, da v primeru neuspelega napada uporabi drugačen način izvedbe napada. Tovrstni napadi napadalcu omogočajo, da lahko okužen sistem uporabi tudi kot »oporišče« za izvedbo naslednjih napadov [8,9].

2.3.1 Način delovanja

APT napadi potekajo v več fazah: vdor, odkritje, zajetje in eksfiltracija podatkov. Pred dejansko izvedbo napada pa izvajalci napadov pridobivajo informacije o cilju napada, kar bi lahko označili kot predhodno fazo [11].

2.3.2 Predhodna faza – pridobivanje informacij o cilju napada

Napadalec pred izvedbo napada zbira oz. pridobiva podatke, z uporabo tehnik socialnega inženiringa in tako poizkuša izboljšati učinkovitost napada. V tej fazi je njegov cilj pridobivanje strateško pomembnih podatkov o ciljnem sistemu, kot so: podatki poslovnih aplikacijah in programski opremi organizacije, hierarhijo sistema, odnose med zaposlenimi znotraj organizacije ipd. S pridobljenimi podatki lahko tako napadalec učinkovito sestavi vsebino e-pošte, ki naj bi bila za prejemnika dovolj zanimiva, da bo odprl prejeto priponko ali kliknil na priloženo spletno povezavo [11].

2.3.3 Faza vdora

Nato nastopi faza, v kateri poskuša napadalec vdreti v omrežje organizacije. Za dosego tega cilja lahko napadalci uporabijo različne pristope. Najpogostejša vstopna točka napadalcev je danes najbolj razširjena oblika poslovne komunikacije – e-pošta. Zaradi nizke stopnje vloženega truda in pogoste komunikacije preko e-pošte, napadalec izbrani žrtvi pošlje e-pošto, ki vsebuje priponko z zlonamerno programsko opremo. Takšne priponke so najpogosteje v obliki PDF dokumentov, Microsoft Word, Excel ali PowerPoint dokumentov ter izvršljivih datotek (.exe datoteke). APT napadi se pogosto bazirajo na novi zlonamerni programski opremi t.i. »Zero-Day«, katero požarni zidovi ne zaznajo.

Izvajalci napadov lahko za vstopno točko uporabijo tudi t.i. instant sporočila ali socialna omrežja, s katerimi pritegnejo potencialno tarčo in jo (pod pretvezo) pripravijo, da klikne na priloženo povezavo ali da prenese datoteko, ki vsebuje zlonamerno programsko opremo.

Za pošiljanje elektronske pošte tarčam izvrševalci napadov uporabljajo lažne elektronske naslove ali e-naslove organizacij ali oseb, s katerimi je tarča napada v preteklosti že komunicirala, saj tako povečajo možnost za realizacijo napada.

Ko žrtev odpre priloženi dokument, se trojanski konj zažene in naloži na računalnik ter tako napadalcu omogoči oddaljen dostop in nadzor nad okuženim sistemom [8, 9].

2.3.4 Faza odkrivanja

Ko napadalec pridobi dostop do enega izmed računalnikov znotraj sistema, začne ocenjevati omrežje, preučevati strukturo sistema ter na podlagi tega locira pomembne podatke. V fazi odkrivanja je vloga napadalca poiskati ranljivosti napadenega sistema, pridobiti dostop do čim večjega števila podatkov ter seveda ostati v sistemu kar se da dolgo neodkrit in si tako omogočiti dolgoročen dostop do podatkov ciljne organizacije [10].

2.3.5 Faza zajetja

V fazi zajetja napadalec z zlonamerno kodo okuži več naprav znotraj omrežja ciljne organizacije in tako pridobi nadzor nad njimi. Na ta način si zagotovi prikrit dostop do podatkov organizacije, ki jih lahko podrobno analizira in locira zanj pomembne informacije. Le te bo v nadaljevanju poizkušal prenesti izven organizacije [10].

2.3.6 Faza eksfiltracije

Zadnji korak APT napada predstavlja prenos kritičnih informacij nazaj k napadalcu. V fazi eksfiltracije napadalec poišče način, kako ukrasti podatke ciljne organizacije. Izvajalec napada lahko ciljne podatke naloži na oddaljen strežnik ali spletno mesto, do katerega ima dostop. Pri uporabi bolj prikritih metod, pa lahko podatke tudi šifrira in tako dodatno prikrije eksfiltracijo. Eksfiltracijo podatkov lahko napadalec izvede v enem koraku, lahko pa jo izvaja postopoma.

Na tem mestu je potrebno poudariti, da APT napadi praviloma niso izvedeni zgolj v enkratnem procesu, pač pa se cikel odkrivanja, zajemanja in eksfiltracije pogosto ponavlja [10].

2.4 Primer APT napada

Eden bolj znanih primerov APT napadov zadnjih let je zagotovo »EuroGrabber« napad iz leta 2012, s katerim so napadalci ukradli okoli 36 milijonov eurov več kot 30.000 strankam iz več kot 30 bank Italije, Španije, Nemčije in Nizozemske.
Napadalci so za napad uporabili zlonamerno programsko opremo in z njo okužili računalnike ter mobilne naprave strank bank. Napad je koristil tudi SMS sporočila, ki jih banke uporabljajo kot del varnega vpisa in overjanja uporabnikov.
Napad je bil zasnovan tako, da je najprej okužil računalnike in mobilne naprave žrtev, s spremenjeno različico trojanskega konja Zeus. Ko je žrtev poizkušala izvesti spletno bančno transakcijo, jo je trojanski konj prestregel. Pod pretvezo nadgradnje spletne bančne aplikacije, je žrtev pretental v izdajo dodatnih informacij, vključno s telefonsko številko mobilne naprave, da bi jo lahko okužil. Trojanski konj je deloval na Android in Blackberry napravah ter tako omogočil širši obseg napada.
Ko sta bili tako računalnik kot mobilna naprava okuženi, je lahko napadalec prestregel in se polastil vseh bančnih transakcij žrtve, vključno s ključem za dokončanje transakcije: SMS banke stranki, ki vključuje avtentikacijsko številko transakcije (Transaction authentication number - TAN). S številko računa, geslom ter TAN številko, so lahko napadalci na skrivaj izvajali prenose sredstev iz računov žrtev medtem, ko so žrtve imele vtis, da je njihova transakcija uspešno zaključena.
Prizadeti so bili bančni uporabniki v podjetjih, kot tudi zasebni. Pri posameznem napadu so se izvajali samodejni prenosi sredstev, v višini med 500 in 250.000 euri na račune, razpršene po vsej Evropi.
Napad je vključeval 10 stopenj, začel pa se je z okužbo z modificirano verzijo trojanskega konja Zeus:

- računalnik žrtve se je okužil z nenamenskim obiskom okužene spletne strani ali z klikom na povezavo iz »Phishing« elektronskega poštnega sporočila,
- uporabniki so nato obiskali spletno stran svoje banke ter se prijavile v svoj račun,
- modificiran trojanski konj Zeus je vbrizgal zlonamerno kodo v spletno stran banke vključno z zahtevo, da uporabnik vnese informacije o številki ter operacijskem sistemu na mobilni napravi,
- ti podatki so bili preko interneta poslani v napadalčevo cono odlaganja (ang. Drop Zone), kjer so se hranili,

- strežnik napadalca je uporabniku poslal SMS sporočilo, s povezavo do trojanskega konja za mobilne naprave – eno izmed verzij Zitmo trojanskega konja,
- v SMS sporočilu je bilo navodilo, naj klikne na povezavo z namenom »posodobitve varnosti spletnega bančnega sistema«. Ob kliku se je na mobilno napravo namestil mobilni trojanski konj in tako dopolnil sistem,
- od takrat se je ob vsaki prijavi uporabnika v svoj bančni račun sprožil trojanski konj in izvedel samodejni prenos denarja iz računa žrtve z uporabo njenih pravih poverilnic,
- za dokončanje prenosa banka pošlje SMS uporabniku s TAN številko, ki pa jo trojanski konj na mobilni napravi pošlje strežniku napadalca,
- prilagojeni Zeus trojanski konj na računalniku uporabnika prejme TAN številko,
- napadalec je prenesel sredstva iz bančnega računa žrtve in Eurograbber, napad se je zaključil [11].

3. Požarni zid

Požarni zid deluje kot pregrada med zaupanja vrednem omrežjem ter ostalimi omrežji, kot je internet. Požarni zid nadzira dostop do virov znotraj omrežja, s pozitivnim modelom kontrole. To pomeni, da je dovoljen samo točno definiran omrežni promet, ves ostali promet pa je zavrnjen.
Izraz požarni zid je izposojen iz procesa gašenja in preprečevanja požarov, kjer se požarni zid uporablja kot ovira za preprečevanje širjenja požara.
Ko se je v računalništvu začel opuščati model osrednjega računalnika (Mainframe) in uporabljati model odjemalec−strežnik, se je pojavila tudi potreba po nadzoru dostopa do strežnika. Pred pojavom požarnih zidov, konec osemdesetih let, so edino pravo obliko omrežne varnosti predstavljali seznami za nadzor dostopa ACL (Access Control List). ACL seznami so določali, katerim IP naslovom se odobri dostop do omrežja in katerim ne.
Hitro širjenje interneta in posledično večja povezljivost med omrežji, je botrovala k temu, da ta vrsta filtriranja prometa ni bila več dovolj za uspešno zaščito sistema, saj so v glavi (Header) paketa le osnovne informacije. Digital Equipment Corp. je leta 1992 izdal na trg prvi komercialni požarni zid DAC SEAL. Od tistega dne se tehnologija požarnih zidov nenehno razvija, da bi lahko kljubovala hitremu naraščanju sofisticiranih kibernetskih napadov [12].

3.1 Principi delovanja požarnega zidu

3.1.1 Referenčni TCP/IP model

TCP/IP je kratica za Transmission Control Protocol in Internet Protocol. To je model, ki se uporablja v trenutni arhitekturi interneta. Protokoli so skupek pravil, ki urejajo celotno komunikacijo preko omrežja. Ti protokoli opisujejo gibanje podatkov med izvorom in ciljem ter tudi vso komunikacijo na internetu.
TCP/IP so razvili na Ministrstvu za obrambo Združenih držav Amerike, kot del projekta za raziskovanje omrežnih povezav, z namenom povezovanja oddaljenih naprav med seboj. Principom, katerim so sledili, in ki so pripeljali do TCP/IP modela so:

- podpora prilagodljivi arhitekturi – dodajanje novih naprav v omrežje je bilo enostavno,
- omrežje je bilo robustno in odporno na napake. Povezave se, dokler so naprave delovale, niso prekinile.

Osnovna ideja pri razvoju je bila omogočiti aplikaciji na enem računalniku komunikacijo (pošiljanje paketov) drugi aplikaciji, ki teče na drugem računalniku [13].

TCP/IP model je sestavljen iz štirih slojev [14]:

Povezovalni sloj – označuje podrobnosti, kako se podatki fizično prenašajo preko omrežja, vključno s tem, kako naprave neposredno povezane na mrežni medij (koaksialni kabel, bakreni kabel, optični kabel) signalizirajo bite.
Uporabljeni protokoli na tem sloju so: *Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.*

Internetni sloj – definira podrobnosti združevanja paketov v IP okvirje, ki vsebujejo informacijo o izvornem in ciljnem IP naslovu. Te informacije se nato uporabijo za posredovanje okvirjev po omrežju. Izvaja tudi usmerjanje IP okvirjev.
Uporabljeni protokoli na tem sloju so: *IP, ICMP, ARP, RARP.*

Transportni sloj - omogoča upravljanje komunikacijske seje med računalniki. Določa raven storitev in stanje povezave, ki se uporablja pri prenosu podatkov.
Uporabljeni protokoli na tem sloju so: *TCP, UDP, RTP.*

Aplikacijski sloj - določa protokole TCP/IP aplikacij in definira kako programi komunicirajo s transportnim slojem za uporabo omrežja.
Uporabljeni protokoli na tem sloju so: *HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows*, drugi uporabniški protokoli.

3.1.2 NAT - prevajanje omrežnega naslova

NAT (Network Address Translation) ali prevajanje omrežnega naslova, je metoda preslikave enega IP naslova v drugega, s spremembo informacije o IP naslovu v glavi IP okvirjev, medtem ko prečkajo napravo za usmerjanje prometa. Zaradi pomanjkanja javnih oz. IP naslovov, ki so primerni za usmerjanje na internetu, je danes ključnega pomena, saj omogoča komunikacijo vsem računalnikom iz določenega lokalnega omrežja v internet, preko enega IP naslova. Tako bistveno pripomore k ohranjanju svetovnega naslovnega prostora [15].
NAT izvaja naprava, ki je postavljena na rob med lokalnim omrežjem in internetom. Ker je v večini današnjih omrežij to požarni zid, je to osnovna funkcionalnost vseh požarnih zidov.

3.1.3 Paketno filtriranje

Prvotni požarni zidovi so delovali s pomočjo paketnega filtriranja. Paketni filtri delujejo z vpogledom v "pakete", ki se prenašajo med računalniki na internetu. Če se paket ne ujema s pravili paketnega filtra, bo filter le tega zavrgel. Nasprotno, če se paket ujema z enim ali več

programiranimi filtri, ga požarni zid spusti v omrežje. Ta vrsta filtriranja se ne zmeni, ali je paket del obstoječega toka prometa – ne shranjuje nobene informacije o stanju povezave. Filtriranje paketov temelji le na informacijah vsebovanih v samem okvirju paketa (najpogosteje je to kombinacija izvornega in ciljnega IP naslova, protokola, TCP ali UDP prometa ter številke vrat). Deluje na omrežnem sloju.

3.1.4 »Stateful inspection« ali kontrola s stanji

Stateful inspection, znan tudi kot dinamično paketno filtriranje. Je tehnologija požarnih zidov, ki spremlja stanje aktivnih povezav, ko prečkajo požarni zid in uporabi te informacije za določanje, katere omrežne pakete spustiti skozi požarni zid.
Stateful inspection je v veliki meri nadomestil starejšo tehnologijo statičnega paketnega filtriranja. Pri statičnem paketnem filtriranju je požarni zid pregledal samo glavo IP paketa. Požarni zid uporablja ta način pregledovanja, da lahko spremlja trenutno aktivne povezave. Stateful inspection beleži informacije o izvornem in ciljnem IP naslovu, vratom, aplikacijah in druge informacije o povezavi.
Na primer, če je na požarnem zidu pravilo, ki računalniku omogoča povezovanje na spletni strežnik, si požarni zid zabeleži podatke o povezavi. Ko strežnik odgovori, požarni zid zazna, da se pričakuje odgovor iz spletnega strežnika na računalnik. Odgovor spusti skozi požarni zid brez pregledovana baze varnostnih pravil. Varnostno pravilo mora omogočati začetni odhodni promet in takrat si požarni zid zapiše povezavo v tabelo povezav [16].

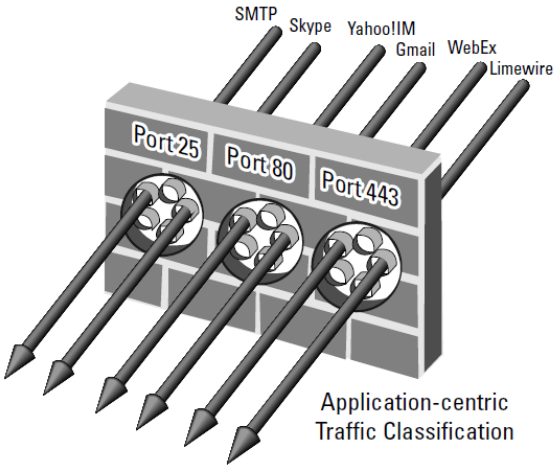
3.2 Požarni zidovi naslednje generacije

Požarni zid naslednje generacije (NGFW – Next Generation Firewall) je požarni zid, ki je sposoben odkriti in blokirati napredne napade, z uporabo varnostnih politik na ravni aplikacij, kot tudi na ravni vrat in protokolov.
Požarni zidovi naslednje generacije združujejo tri ključne vidike: visoko zmogljivost, sistem za preprečevanje vdorov (IPS) in nadzor nad aplikacijami. Podobno kot uvedba »stateful inspection-a« pri prvi generaciji požarnih zidov, prinašajo tudi požarni zidovi naslednje generacije dodatno dimenzijo v procesu odločanja požarnega zidu. S sposobnostjo podrobne analize in razumevanja prometa, lahko sprejme učinkovite ukrepe za blokiranje prometa in tako prepreči izrabo ranljivosti.
Požarni zidovi naslednje generacije združujejo zmogljivosti tradicionalnih požarnih zidov − vključno s paketnim filtriranjem, prevajanjem omrežnih naslovov (NAT), blokiranjem URL strani, s funkcionalnostmi in lastnostmi, ki jih pri tradicionalnih požarnih zidovih ne najdemo. Te vključujejo sistem za preprečevanje vdorov (IPS), pregled in dešifriranje SSL protokola, globoko analizo paketov, detekcijo zlonamerne programske opreme in razpoznavanje aplikacij.

Ta tehnologij je bila razvita z namenom preprečevanja vse večjega števila groženj in napadov, ki se odvijajo na aplikacijski plasti TCP/IP referenčnega modela [17,18].

3.2.1 Razpoznavanje aplikacij

Največja razlika med tradicionalnimi požarnimi zidovi in NGFW je dejstvo, da se slednji zavedajo aplikacij. Tradicionalni požarni zidovi se zanašajo le na standardna vrata, ki naj bi jih aplikacija uporabljala in se na podlagi tega odločijo, ali bodo promet dovolili. NGFW ne v naprej domneva, da določena aplikacija uporablja le določena vrata. Sposoben je spremljati promet na vseh plasteh in določiti, kakšna vrsto prometa se pošilja in sprejema. Najpogostejši primer je trenutna uporaba HTTP vrat 80. Tradicionalno se ta vrata uporablja samo za HTTP promet, vendar to ne velja več, še veliko število različnih aplikacij uporablja ta vrata za komunikacijo in prenos podatkov, med končnim uporabnikom in strežnikom. Obstaja več različnih načinov, kako je mogoče ena vrata uporabiti za različne vrste prometa med katerimi je najpogostejše t.i. »*tuneliranje*« aplikacij. Preko tunelov je promet na izvoru skrit v podatkovna polja HTTP paketa in nato odvit na destinaciji. Z vidika tradicionalnega požarnega zidu izgleda ta paket kot preprost HTTP paket spletnega prometa, vendar pa NGFW odkrije njegov pravi namen in ga blokira, še preden doseže cilj [18].



Slika 7: Prikaz razpoznavanja aplikacij ne glede na uporabo določenih vrat.

3.2.2 Razpoznavanje uporabnikov

Še ena velika razlika med tradicionalnimi požarnimi zidovi in NGFW je, da so slednji sposobni določiti identiteto izvora omrežnega prometa – uporabnika ali napravo. To pomeni, da požarni zid poveže IP naslove z uporabniki ter tako omogoča lažje in bolj učinkovito izvrševanje nadzora dovoljenega prometa. Požarni zid se za informacijo o identiteti poveže z obstoječimi sistemi za avtentikacijo v organizaciji (aktivni imenik, LDAP). Na ta način lahko omrežni

administratorji nadzirajo, komu je dovoljena uporaba določenih aplikacij in ne samo, kateri promet je dovoljen ali ne [17].

3.2.3 Protivirusna zaščita in zaščita pred zlonamerno programsko opremo

Požarni zidovi naslednje generacije lahko zaznajo viruse in zlonamerno programsko kodo v prometu, ki je namenjen v omrežje. Na ta način lahko takšen promet blokirajo že na samem začetku prenosa in tako zmanjšajo tveganje okužb računalnikov v sistemu. Večina požarnih zidov naslednje generacije uporablja bazo virusnih definicij znanih proizvajalcev protivirusnih programov, nekatera podjetja pa vzdržujejo lastno bazo.

3.2.4 Napredni IPS sistem

IPS (Intrusion Prevention System) ali sistem za preprečevanje vdorov je odgovoren za odkrivanje napadov. Zaznava napadov temelji na več različnih tehnikah, vključno z uporabo podpisov groženj, definicij znanih napadov z izkoriščanjem, zaznavo nenavadnih omrežnih aktivnost in vedenjsko analizo prometa.

V sistemu, kjer je nameščen tradicionalni požarni zid, je pogosto poleg požarnega zidu nameščen tudi sistem za zaznavanje vdorov (IDS) ali IPS. Običajno se ta pojavlja kot samostojna naprava ali ločena logična enota znotraj ene naprave. V požarnih zidovih naslednje generacije je IPS sistem popolnoma integriran. IPS funkcionalnost kot taka ni spremenjena, v primerjavi s samostojnim sistemom. Ker pa je v tem primeru povezana z ostalimi naprednimi funkcionalnostmi, in ima tako na razpolago več informacij o samem prometu, je veliko bolj učinkovita, v primerjavi s samostojnim sistemom [17,18].

3.2.5 SSL dešifriranje

Vedno več omrežnega prometa med odjemalci in strežniki poteka po SSL (Secure Socket Layer) standardu, imenovanem tudi sloj varnih vtičnic. Požarni zidovi naslednje generacije lahko takšen promet dešifrirajo in tako preverijo morebitno prisotnost groženj v prometu. To naredijo na način, da delujejo kot vmesni člen (Man in the middle) v komunikaciji med strežnikom in odjemalcem. Na ta način lahko zagotovijo dodatno zaščito pred škodljivimi aplikacijami in aktivnosti, ki jih nekateri skušajo zakriti z uporabo šifriranja. Brez te možnosti požarni zidovi ne bi mogli zaznati groženj v tekem prometu, saj ne bi bili sposobni podrobno analizirati paketov.

3.2.6 »Sandbox« - varnostna analiza datotek v oblaku oziroma peskovnik

Današnji napadalci so se naučili, kako zaobiti razne protivirusne zaščite in zaščite pred vdori, ki temeljijo na bazah definicij in podpisov. Sposobni so hitro spremeniti obnašanje svoje zlonamerne programske opreme in ustvariti t.i. »Zero-day« grožnje. Potreben je bil nov sistem za odkrivanje groženj, ki omogoča da datoteke, s katerimi se požarni zid do sedaj še ni srečal, analiziramo v varnem okolju in ugotovimo, ali nam želijo škodovati. Takšnemu sistemu pravimo Sandbox.

Obstajata dve vrsti neznanih groženj:

- grožnje, ki temeljijo na znanih ranljivosti in se zelo hitro spreminjajo, v nekaj sekundah ali minutah. Nadzor, ki temelji na podpisih, takšnim spremembam ne more slediti;

- grožnje, ki temeljijo na neznanih ali *zero-day* ranljivostih. Tudi pri takšnih grožnjah nima sistem, ki temelji na podpisih, nobene možnosti za odkrivanje in odpravo.

Najboljši način za odkrivanje teh neznanih grožnje je, da datoteke, ki vsebujejo takšne grožnje, zaženemo v varnem in virtualnem okolju. V takšnem okolju je datoteka zagnana pod nadzorom in tako je moč zaznati njeno zlonamerno obnašanje. Ko sistem zazna grožnjo, jo preuči in ustvari podroben opis le te, oziroma »signature« (podpis). S pomočjo teh podpisov bo ta tip napada lahko zaznal in blokiral tudi tradicionalni sistem za preprečevanje vdorov.

Vsi peskovniki niso enako učinkoviti pri zaznavi zlonamernega programske kode. Tudi napadalci so se seznanili s sandbox rešitvami in so sposobni razviti takšno zlonamerno programsko opremo, ki je sposobna zaznati, da se nahaja v peskovniku in se takrat ne izvaja [19].

4. Izvedba testiranj požarnih zidov

4.1 Opis rešitve

S testiranjem želimo ugotoviti ali so požarni zidovi naslednje generacije dovolj zmogljivi, da uspejo zadostiti današnjim potrebam po visokih hitrostih povezovanja v internet ter sočasno poskrbeti za učinkovito zaščito omrežja organizacije pred sodobnimi grožnjami.

Teste smo razdelili v dva logična sklopa: testi prepustnosti ter testi zaščite pred napadi. V prvem sklopu smo opravili naslednje teste:

1) Test prepustnosti požarnih zidov brez vklopa varnostnih funkcionalnosti.
2) Test prepustnosti požarnih zidov ob vklopu NAT funkcionalnosti ter osnovnih varnostnih pravil.
3) Test prepustnosti požarnih zidov ob vklopu funkcionalnosti za razpoznavanje aplikacij.
4) Test prepustnosti požarnih zidov ob vklopu funkcionalnosti za preprečevanje groženj.

V drugem sklopu pa smo opravili naslednja dva testa:

1) Test učinkovitosti zaščite pred DOS napadi.
2) Test učinkovitosti zaščite pred APT napadi.

V nadaljevanju bomo najprej predstavili strojno in programsko opremo, ki smo jo pri testih uporabili. Opisali in grafično predstavili bomo naše testno okolje ter potrebne nastavitve opreme pred začetkom samega testiranja.
Nato bomo vsak test posebej opisali, prikazali potrebne spremembe oz. dodatne nastavitve požarnih zidov ter na koncu vsakega testa podali rezultate testiranja.
V naslednjem poglavju pa bomo rezultate testiranj podrobneje analizirali ter interpretirali razlike v rezultatih med posameznimi požarnimi zidovi.

4.2 Uporabljena strojna in programska oprema

Pri testih požarnih zidov naslednje generacije smo uporabili tri naprave različnih proizvajalcev. Dva izmed njih – »Palo Alto Networks« ter »Check Point Software Technologies« sta po tržnem deležu v samem svetovnem vrhu. Tretji proizvajalec - »Barracuda Networks« pa je relativno novo podjetje na tržišču z majhnim tržnim deležem.

Uporabili smo naslednje modele požarnih zidov omenjenih proizvajalcev:

- Barracuda F380,
- Palo Alto PA-3020,
- Check Point 4600.

Za testiranje prepustnosti požarnih zidov smo uporabili visoko zmogljiv generator omrežnega prometa Agilent Technologies N4190B. Čeprav je proizveden leta 2005, je ta generator še danes tehnološko dovršen izdelek, saj zmore proizvajati do 2 Gbps omrežnega prometa do sedme plasti OSI referenčnega modela. Po naših podatkih je ta Agilent Technologies generator eden izmed redkih oz. edini generator »L7« omrežnega prometa, v lasti katerega izmed slovenskih podjetij.

V nadaljevanju smo vsak požarni zid ter generator omrežnega prometa podrobneje opisali ter predstavili glavne funkcionalnosti vsakega.

4.3 Opis požarnega zidu Barracuda F380

Slika 8: Požarni zid naslednje generacije Barracuda NG F380.

Barracuda F380 je zmogljiv požarni zid naslednje generacije namenjen zaščiti omrežne infrastrukture podjetij. Požarni zid ima 8 RJ45 ethernet vmesnikov hitrosti 1 Gbps, konzolni serijski vmesnik namenjen konfiguraciji požarne pregrade ter dva USB vmesnika za nalaganje programske opreme. Za konfiguracijo pregrade uporabljamo aplikacijo »NextGen Admin«, ki jo bomo pobližje spoznali v naslednjih poglavjih.

Možnosti upravljanja:

- preko aplikacije »NextGen Admin«,
- povezava na CLI preko SSH ali TELNET protokola,
- povezava na CLI preko serijskega vmesnika.

Požarni zid Barracuda F380 omogoča nadzor nad aplikacijami, s sistemom »Barracuda Application Control«. Ta nudi natančno identifikacijo velikega števila protokolov in aplikacij, ki prečkajo omrežje, tudi če le-te uporabljajo napredne tehnike zamegljevanja (ang. Obfuscation), preskakovanja vrat (ang. Porthopping) ali šifriranja. Funkcionalnost »Barracuda Application Control« nudi možnost blokiranja uporabe neželenih programov, nadzira in omejuje porabo dovoljenih aplikacij ter tako hrani pasovno širino podjetja za ključne poslovne aplikacije.
Možnosti spletnega filtriranja na požarnem zidu omogočajo zelo zrnat vpogled v spleto dejavnost v realnem času, razčlenjeno po posameznih uporabnikih in aplikacijah. Skrbniki omrežij lahko z blokiranjem dostopa do nezaželenih spletnih strani in strežnikov ustvarijo učinkovite politike uporabe internetnih virov, ustavijo prenose neželene programske opreme in ostalih spletnih groženj.
Vgrajeni sistem za zaznavanje in preprečevanje vdorov (IDS / IPS) povečuje varnost omrežja z zagotavljanjem popolne in celovite zaščite pred velikim številom groženj, ranljivosti ter izpostavljenosti operacijskih sistemov in aplikacij v realnem času. Tako preprečuje napade kot so:

- SQL vbrizgi in samodejni zagon programske kode,
- poizkusi pridobivanja dostopa in višanja privilegijev,
- napadi na spletno stran z vrinjenjem zlonamerne kode, napisane v skriptnem jeziku,
- napadi z preplavljanjem medpomnilnika,
- DoS and DDoS napadi,
- »Directory traversal« napadi,
- napadi z preiskovanjem in pregledovanjem,
- »Backdoor« napadi,
- trojanskimi konji, virusi, črvi »rootkit-i« in vohunsko programsko opremo.

Z zagotavljanjem napredne zaščite pred grožnjami in napadi, kot so zaščita pred segmentacijo toka in paketno anomalijo, »TCP split handshake« zaščita, IP in RPC defregmentacija, zaščita pred FTP vdori kot tudi URL in HTML dekodiranje, je požarna pregrada naslednje generacije Barracuda F380 sposobna identificirati in blokirati napredne poskuse evazije in tehnike zamegljevanja, ki jih napadalci uporabljajo za izogibanje tradicionalnih sistemov za preprečevanje vdorov.
Samodejno posodabljanje baze podpisov groženj na požarnem zidu se izvaja po rednem urniku ali na podlagi izrednih dogodkov. S tem zagotovimo, da je Barracuda požarni zid vedno posodobljena.
Zaščita pred zlonamerno programsko opremo ščiti notranje omrežje organizacije, s skeniranjem spletne vsebine (HTTP in HTTPS), e-pošte (SMTP, POP3) in prenosi datotek (FTP), preko dveh popolnoma integriranih protivirusnih sistemov. Zaščita pred zlonamerno programsko opremo temelji na rednih posodobitvah podpisov kot tudi napredni hevristiki za odkrivanje neželenih programov, še preden so novi podpisi na razpolago.
Zaščita pred zlonamerno programsko opremo zajema viruse, črve, trojanske konje, zlonamerne Java aplikacije in programe. Uporablja znane tehnike izkoriščanja PDF datotek, slik in pisarniških dokumentov ter makro virusov, tudi če le-te uporabljajo tehnike za prikrivanje in evazijo.

Požarna pregrada ima funkcionalnost napredne zaznave groženj »Advanced Threat Detection«, ki nudi zašito pred napredno zlonamerno programsko opremo, »zero-day« grožnjami in usmerjenimi kibernetskimi napadi, ki jih protivirusni oz. sistem za preprečevanje vdorov ne zazna. ATD analizira datoteko v »Barracuda ATD« storitvi v oblaku in ji dodeli določeno oceno stopnje tveganosti. Lokalne politike požarnega zidu nato določajo, kako ravnati z datotekami, ki so ovrednotene z nizko, srednje ali visoko stopnjo tveganosti. Sistem lahko

obvesti administratorja po elektronski pošti oz. uporabi eno izmed samodejnih varnostnih politik. V ATD oblak lahko pošljemo tudi lokalne datoteke preko aplikacije »NextGenAdmin« [20].

4.3.1 Specifikacije požarnega zidu Barracuda F380

- prepustnost požarnega zidu (merjeno z veliki paketi MTU 1500) 3,8 Gbps,
- IPS prepustnost 1,4 Gbps,
- prepustnost VPN povezav 1,2 Mbps,
- največje sočasno število sej 400.000,
- največje število na novo vzpostavljenih sej na sekundo 15.000,
- 8 Gigabitnih ethernet RJ45 vmesnikov,
- 2 USB 2.0 vmesnika,
- en serijski konzolni vmesnik RJ45,
- RAM spomin 4 GB,
- SSD disk 80 GB.

4.4 Opis požarnega zidu Palo Alto PA-3020

Slika 9: Požarni zid naslednje generacije Palo Alto Networks PA-3020.

PA-3020 proizvajalca Palo Alto Networks je zmogljiv požarni zid naslednje generacije, z 12 ethernet vmesniki, hitrosti 1 Gbps ter 8 Ethernet SFP vmesniki, ločenim RJ45 ethernet vmesnik za nadzor, konzolnim serijskim vmesnikom namenjenim konfiguraciji požarne pregrade, USB vmesnikom za nalaganje programske opreme ter dvema vmesnikoma, ki sta namenjena za postavitev v visoko redundantnem načinu.
Možnosti upravljanja:

- preko spletnega uporabniškega vmesnika,
- preko aplikacije Panorama,
- povezava na CLI preko SSH ali TELNET protokola,
- povezava na CLI preko serijskega vmesnika.

»Palo Alto Networks App-ID ™« je patentirana tehnologija klasifikacije prometa, ki razpozna aplikacije v omrežju ne glede na vrata, protokol, uporabo SSL šifriranja in tehnik izmikanja. To doseže z uporabo različnih tehnik, kot so: uporaba podpisov, dešifriranje (če je potrebno), dekodiranje protokolov in hevrisitke. Razumevanje in uporaba varnostne politike nad aplikacijami, ki se pretakajo v omrežju, je bolj intuitiven, napreden in uporaben pristop k varnosti, za razliko od tradicionalnih požarnih zidov, katerih politike temeljijo zgolj na omejevanju prometa po vratih. Skupaj s funkcionalnostjo identifikacije uporabnika (»User-ID ™«), »App-ID« omogoča implementacijo t.i. "pozitivnega modela" varnosti, ki jasno opredeljuje, kateri uporabniki lahko uporabljajo katere aplikacije, v skladu s poslovnimi zahtevami. »App-ID« je vedno vklopljen ter zagotavlja podrobno prepoznavnost aplikacij v prometu, ki prečka požarni zid. »App-ID« temelji na zbirki podatkov, ki vsebuje več kot dva tisoč aplikacij in v katero je tedensko dodanih tri do pet novih aplikacij.
»User-ID™« je tudi patentirana tehnologija, ki povezuje identiteto uporabnika s prometom, ki se pretaka v omrežju. Poleg same identitete uporabnika, lahko določi tudi uporabniško skupino, v katero spada. Na ta način lahko uporabimo varnostne politike, ki niso vezane zgolj na IP

naslove temveč na posamezne uporabniške skupine. Razpoznavanje uporabnikov dosežemo s pregledovanjem dnevnika dogodkov uporabniškega imenika, ki se uporablja (npr. Microsoft Exchange, aktivni imenik, krmilniki brezžičnega prometa). Članstvo v uporabniški skupini se običajno določi z LDAP integracijo v različne imenike (vključno z aktivnim imenikom). Informacija o uporabnikih se tako lahko uporabi pri vseh funkcionalnostih požarnega zidu.
Tehnologija »Content-ID™« skrbi za zaznavanje in blokiranje groženj v vseh aplikacijah in protokolih, ne glede na uporabo tehnik izmikanja. Omrežje ščiti pred zlorabami ranljivosti, zlonamerno programsko opremo in prometom za vodenje in nadzor, ki ga ta ustvari. Tehnologija za preprečevanje ogroženosti vključuje:
IPS - IPS funkcionalnost blokira zlorabe ranljivosti, preplavljanja pomnilnika ter skeniranja vrat. Naprednejše zmogljivosti, kot so blokiranje neveljavnih ali nerazpoznavnih IP paketov, IP defragmentacija in ponovna sestava TCP paketa, ščitijo pred metodami izmikanja in zamegljevanja, ki jih napadalci uporabljajo.
»Anti-Malware« – blokira znano zlonamerno programsko opremo, kot tudi napredne različice znane zlonamerne programske opreme. Zaščita za neznano zlonamerno programsko opremo je na voljo v manj kot petnajstih minutah, preko storitve varnostne analize neznanih datotek v oblaku »Wildfire«.
Upravljanje in nadzor – blokira vso izhodno komunikacijo zlonamerne programske opreme in tudi pasivno analizira DNS poizvedbe ter tako opredeli edinstvene vzorce »botnet« omrežij. Tako izolira okužene uporabnike ter preprečuje sekundarne prenose datotek in podatkov iz podjetja.
URL filtriranje − integrirana baza podatkov za URL filtriranje, omogoča uporabo enostavnih in učinkovitih politik za brskanje po spletu, kot tudi zmanjšuje število okužb z zlonamerno programsko opremo, z blokiranjem dostopa do znanih spletnih strani z zlonamerno programsko opremo ter »phishing« strani.

Filtriranje datotek in podatkov − filtriranje podatkov omogoča izvajanje politik, ki zmanjšujejo tveganje povezano s prenosom nedovoljenih datotek in podatkov. Te politike so:

- blokiranje datoteke glede na vrsto,
- filtriranje podatkov za nadzor prenosa občutljivih podatkov, vključno s številkami kreditnih kartic in socialnega zavarovanja v vsebini prijave ali prilog,
- kontrola prenosov datotek, ki omogoča nadzor prenosov datotek znotraj posamezne aplikacije. Na ta način lahko omogočimo uporabo aplikacije kateri preprečimo neželenih prenose datotek [21].

4.4.1 Specifikacije požarnega zidu PA-3020

- prepustnost požarnega zidu (merjeno z veliki paketi MTU 1500) 2 Gbps (z vključeno funkcionalnostjo razpoznavanja aplikacij),
- prepustnost z vključeno funkcionalnostjo preprečevanja groženj 1 Gbps,
- prepustnost VPN povezav 500 Mbps,
- največje sočasno število sej 250.000,
- največje število na novo vzpostavljenih sej na sekundo 50.000,
- 12 Gigabitnih ethernet RJ45 vmesnikov,
- 8 Gigabitnih SFP vmesnikov,
- 1 Gigabitni RJ45 vmesnik za upravljanje,
- 2 Gigabitna RJ45 vmesnika, namenjena postaviti v visoko redundantnem načinu,
- En serijski konzolni vmesnik RJ45,
- 1 USB 2.0 vmesnik,
- RAM spomin 4 GB,
- SSD disk 120 GB.

4.5 Opis požarnega zidu CheckPoint 4600

Slika 10: Požarni zid naslednje generacije Check Point 4600.

Check Point 4600 požarni zid naslednje generacije je opremljen z osmimi ethernet vmesniki, hitrosti 1 Gbps, konzolnim serijskim vmesnikom, namenjenim konfiguraciji požarne pregrade ter dvema USB vmesnikoma za nalaganje programske opreme. Opcijsko lahko dodamo še štiri 1 Gbps ethernet vmesniki oz. štiri 1 Gbps SFP vmesnike.
Možnosti upravljanja:

- preko aplikacije CheckPoint SmartConsole,
- povezava na CLI preko SSH ali TELNET protokola nudi okrnjeno upravljanje požarnega zidu (sistemske nastavitve, omrežne nastavitve, nastavitve delovanja v visoki razpoložljivosti ter nastavitve vzdrževanja),
- povezava preko spletnega uporabniškega vmesnika nudi okrnjeno upravljanje požarnega zidu (sistemske nastavitve, omrežne nastavitve, nastavitve delovanja v visoki razpoložljivosti ter nastavitve vzdrževanja),
- povezava na CLI, preko serijskega vmesnika.

Check Point 4600 zagotavlja celovito zaščito pred grožnjami s sledečimi tehnologijami:
»SandBlast Threat Emulation« − preprečuje okužbe pred »zero-day« in ciljnimi napadi. Nudi prenos in zagon datotek v virtualnem peskovniku, kjer se datoteke analizira in odkrije morebitno škodljivo obnašanje ter nato prepreči prenos datoteke v omrežje. »Threat extraction« funkcionalnost lahko izloči nevarne dele datotek, kot so aktivne vsebine in vgrajeni objekti za odpravo potencialnih nevarnosti, rekonstruira datoteke ter dostavi sanirano vsebino uporabniku. »Antivirus« – ustavi dohodne zlonamerne datoteke že na prehodu in zagotovi, da ne prizadenejo uporabnikov. Uporablja se baza podatkov o grožnjah »Threat Cloud«, ki vsebuje v realnem času posodobljeno zbirko podpisov virusov ter anomalij. Baza vsebuje tudi podatke o več kot 4,5 milijona podpisov zlonamerne programske opreme ter 300.000 zlonamernih spletnih strani.

»Intrusion Prevention System (IPS)« – zagotavlja popolno in proaktivno zaščito pred vdori, s prednostjo enotne točke upravljanja. Ustrezno dopolnjuje funkcije požarnega zidu, z analizo paketov, ki prečkajo omrežje.
»URL Filtering« – nadzira dostop do več milijonov spletnih strani, razporejenih po kategorijah in omogoča oblikovanje politik dostopa za uporabnike, uporabniške skupine ter kategorije spletnih strani. IT upravljalci lahko blokirajo dostop do določenih spletnih naslovov, posameznih spletnih strani znotraj naslova ter določajo pravila dostopa glede na urnik in dovoljeno porabo pasovne širine.
»SmartLog« − vsi varnostno obveščevalni podatki se zbirajo v naprednem analizatorju dnevnikov dogodkov in tako tvorijo varnostno inteligenco, ki ponuja vpogled v realnem času, v vse dogodke v omrežju.
» Anti-Bot« – zazna »BOT« okužene naprave, preprečuje BOT škodo, z blokiranjem komunikacije napadalcev do centra za upravljanje in nadzor. Baza podatkov o grožnjah se nenehno posodablja iz »ThreadCloud« oblačne baze podatkov.
»Application Control« – nadzoruje dostop do več kot 5.200 aplikacij in 240.000 pripomočkov socialnih omrežij. Omogoča ustvarjanje granularnih varnostnih politik, vezanih na uporabnike oz. uporabniške skupine za blokiranje ali omejevanje uporabe spletnih aplikacij in pripomočkov, kot so takojšnje sporočanje, družbena omrežja, pretakanje video vsebin ter iger.
»Identity Awareness« – prepoznavanje uporabnikov, uporabniških skupin in naprav za ustvarjanje natančnih varnostnih politik, ki temeljijo na identiteti [22].

4.5.1 Specifikacije požarnega zidu Check Point 4600

- Prepustnost požarnega zidu 3,4 Gbps
- Prepustnost z vključeno IPS funkcionalnostjo 630 Mbps
- Prepustnost VPN povezav 1,5 Gbps
- Največje sočasno število sej 1.200.000
- Največje število na novo vzpostavljenih sej na sekundo 50.000
- 8 do 12 Gigabitnih ethernet RJ45 vmesnikov
- Do 4 Gigabitnih SFP vmesnikov
- En serijski konzolni vmesnik RJ45
- dva USB 2.0 vmesnika
- RAM spomin 4 GB
- SSD disk 250 GB

4.6 Opis generatorja omrežnega prometa Agilent Technologies N4190B

Slika 11: Generator omrežnega prometa Agilent Technologies N4190B.

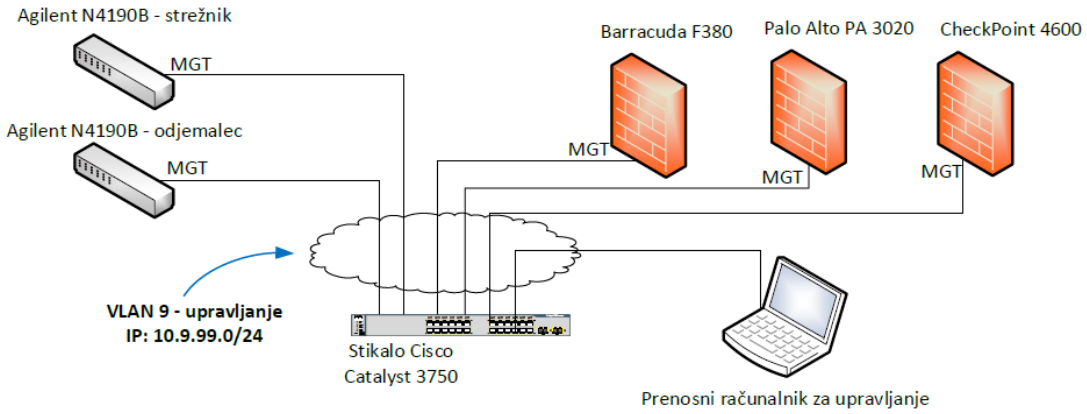
Generator omrežnega prometa Agilent N4190B je opremljen z dvema ethernet vmesnikoma hitrosti 1 Gbps, ločenim RJ45 ethernet vmesnik za nadzor ter konzolnim serijskim vmesnikom, namenjenim konfiguraciji omrežnega generatorja.
Možnosti upravljanja:

- vse nastavitve testov kot tudi proženje samih testov, se izvajajo preko aplikacije »NetPressure«,
- s povezavo na CLI preko serijskega lahko napravi nastavimo samo IP naslov za upravljanje ter še nekaj osnovnih parametrov (hitrost in duplex način vrat …).

Generator lahko proizvede do 2Gbps omrežnega prometa, na vsakih vratih po 1Gbps.
Proizvaja promet od četrte – transportne plasti OSI referenčnega modela, pa vse do sedme – aplikacijske plasti. Na ta način lahko ustvari promet primerljiv tistemu, ki ga ustvarjajo uporabniki pri povezovanju v internet. Uporabljajo ga predvsem proizvajalci omrežne opreme in ponudniki storitev [23].

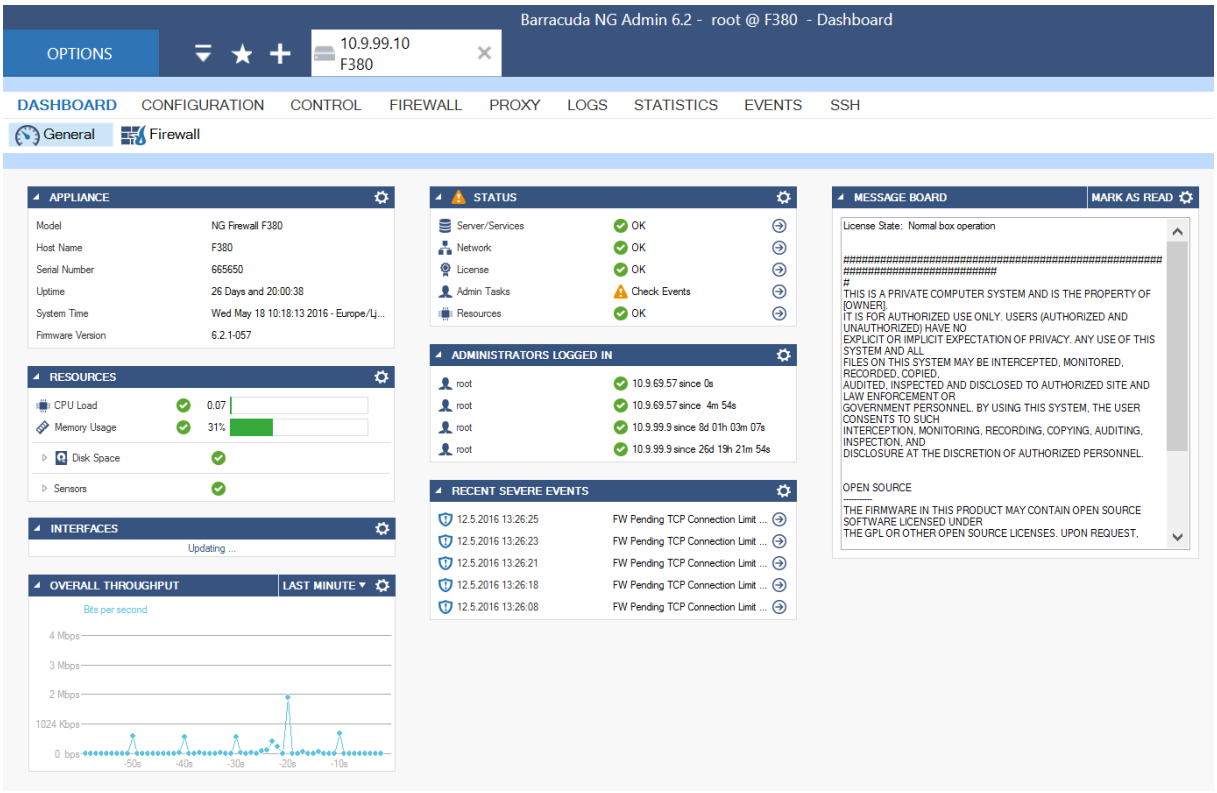
4.7 Opis testnega okolja

Najprej smo na vseh napravah, ki smo jih uporabili pri testiranju, pripravili ločena vrata namenjena upravljanju. Dodelili smo jim ustrezni IP naslov v upravljalnem podomrežju 10.9.99.0/24 ter jih povezali na stikalo. Na stikalu smo ustvarili VLAN 9 in vsa vrata namenjena upravljanju dodelili temu VLAN-u.



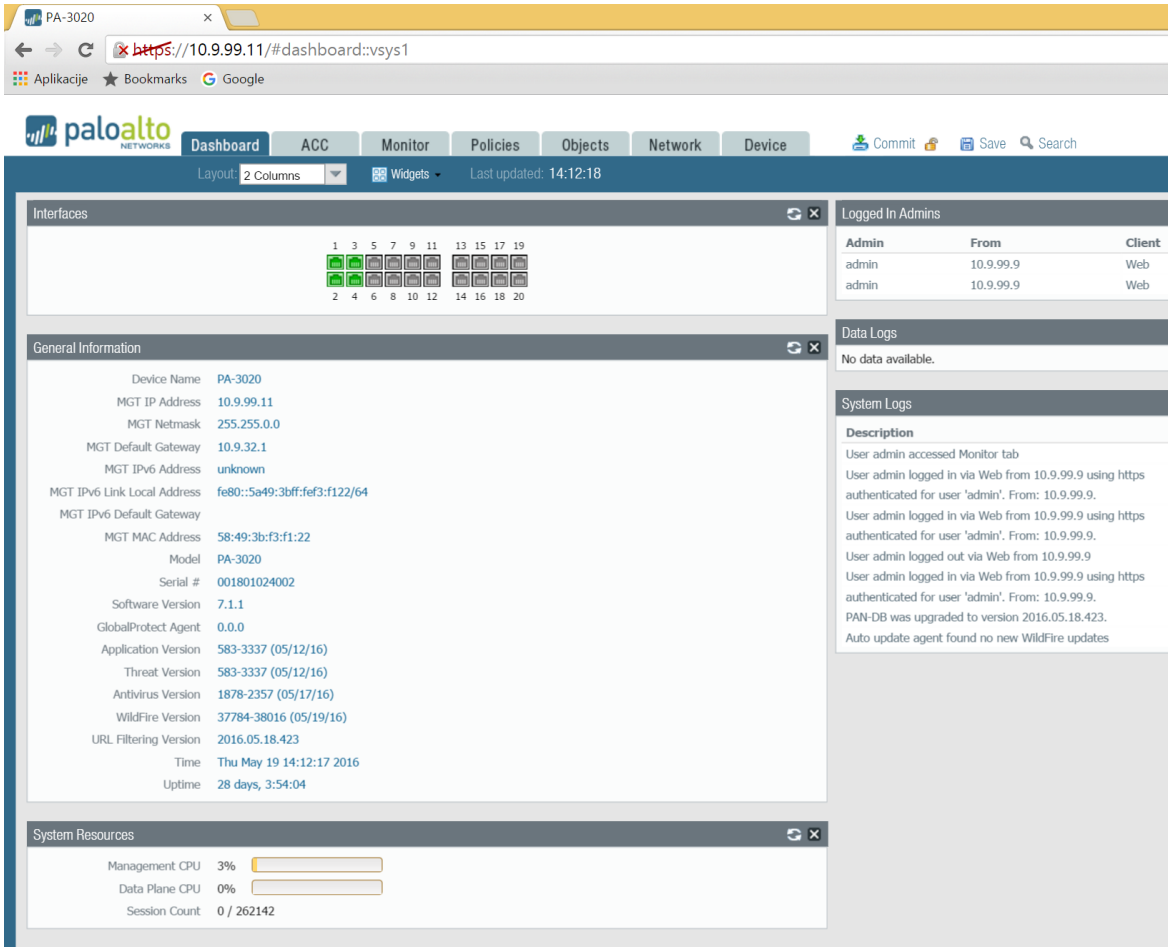
Slika 12: Shema vezave upravljalnih vrat požarnih zidov ter generatorjev omrežnega prometa.

Požarne zidove smo upravljali preko različnih orodij. Požarni zid Barracuda F380 smo po večini upravljali preko namenske aplikacije za upravljanje »Barracuda NextGen Admin«. Izjema so bili izpisi števila sej pri enem izmed testov, ki pa smo jih izvedli preko CLI ukazne vrstice.



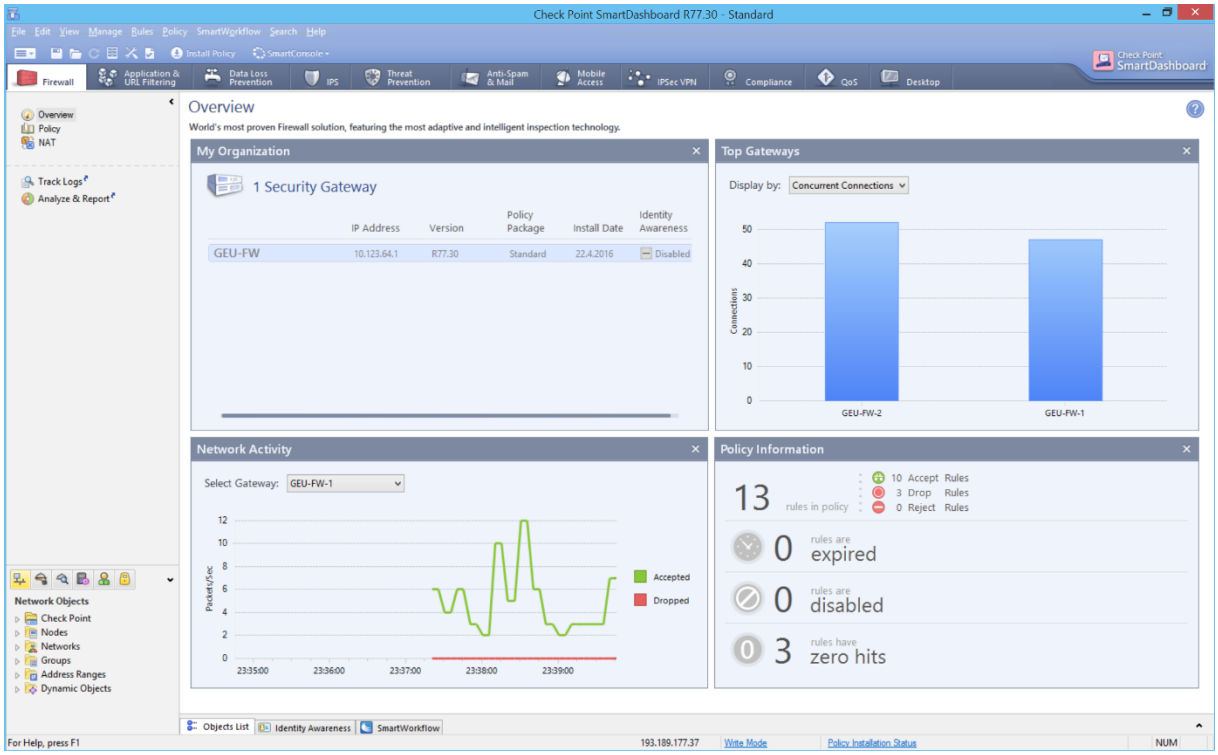
Slika 13: Uporabniški vmesnik za upravljanje požarnega zidu Barracuda F380 – »NG Admin«.

Požarni zid Palo Alto PA-3020 smo upravljali preko spletnega brskalnika, s povezavo na spletni uporabniški vmesnik požarnega zidu. Tudi požarni zid PA omogoča lažje prikazovanje določenih informacij preko CLI ukazne vrstice. Kot bo razvidno v nadaljevanju, smo se tega načina povezovanja poslužili pri enem izmed testov.



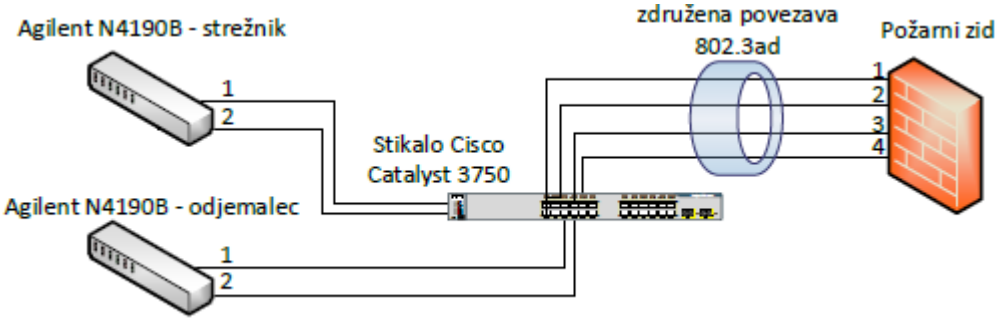
Slika 14: Spletni uporabniški vmesnik za upravljanje požarnega zidu Palo Alto PA-3020.

Požarni zid Check Point 4600 tudi ponuja namensko aplikacijo za upravljanje »Check Point SmartDashboard«, preko katere pa ni možno spreminjati vseh nastavitev. Zato smo za upravljanje in namestitev tega požarnega zidu uporabljali tako »Smart Dashboard«, kot tudi SSH povezavo na CLI uporabniški vmesnik.



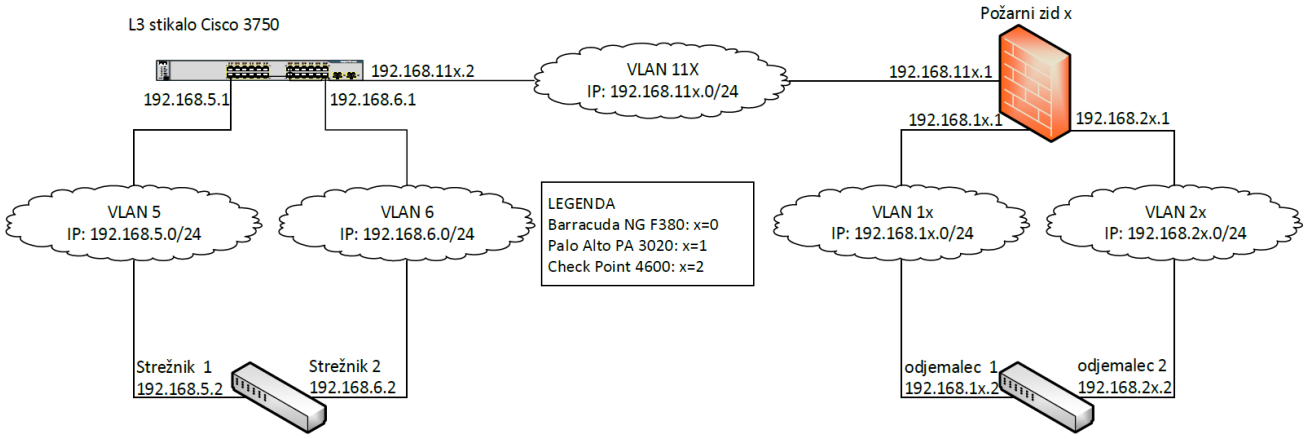
Slika 15: Uporabniški vmesnik za upravljanje požarnega zidu CheckPoint 4600 »SmartDashboard«,

Vse požarne zidove v testnem okolju smo povezali na enak način. Prva štiri vrata požarnega zidu smo združili v eno logično povezavo, s protokolom za združevanje povezav 802.3ad. Enako smo storili za štiri vrata na stikalu, ki so povezana s posameznim požarnim zidom. Na stikalo smo priključili še oba ethernet vmesnika na posameznem generatorju omrežnega prometa – strežniku ter odjemalcu. Ker je vsak vmesnik na generatorju ločena instanca za generiranje prometa, smo jih poimenovali strežnik 1, strežnik 2, odjemalec 1 in odjemalec 2.



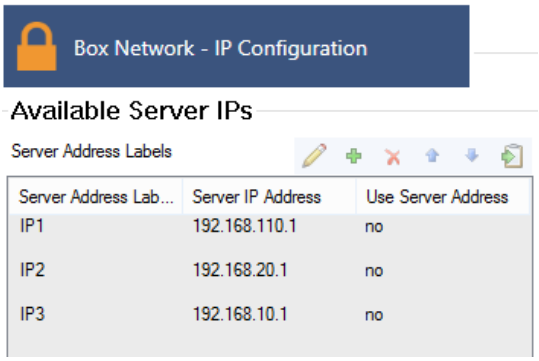
Slika 16: Shema fizične vezave požarnih zidov ter generatorjev omrežnega prometa.

Na stikalu smo pripravili dva VLAN-a: 5 in 6, za povezavo do strežniških generatorjev prometa. Nato smo pripravili še po 3 VLAN-e za vsak požarni zid na testiranju. V VLAN 1x in 2x smo umestili oba odjemalca, ter 11x za povezavo med stikalom ter požarnim zidom (x predstavlja zaporedno številko požarnega zidu na testu). Nato smo namestili ustrezne IP naslove na VLAN-e ter nastavili usmerjanje po sledeči shemi.

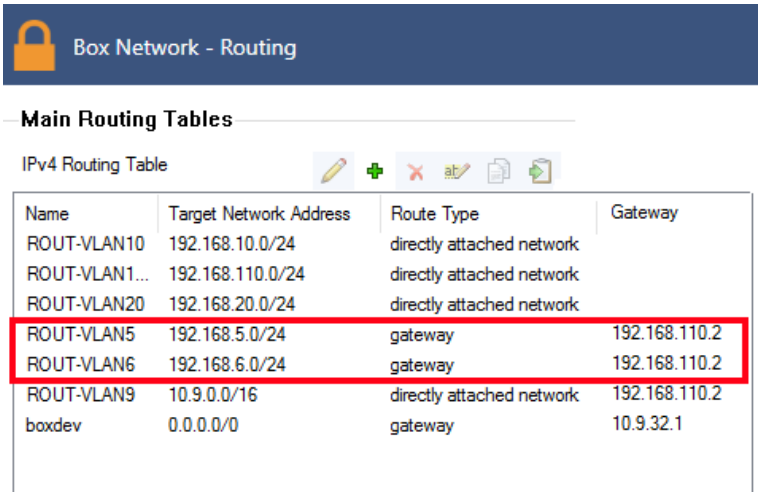


Slika 17: Shema usmerjanja med požarnimi zidovi ter generatorji omrežnega prometa.

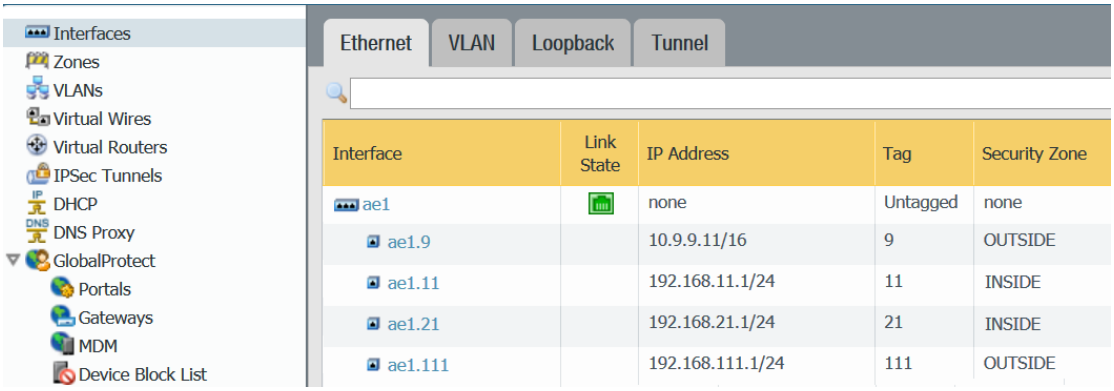
Na posamezni požarni pregradi smo najprej nastavili pripadajoče IP naslove na posamezna vrata ter ustrezno nastavili usmerjanje prometa med strežniškimi in odjemalskimi omrežji.



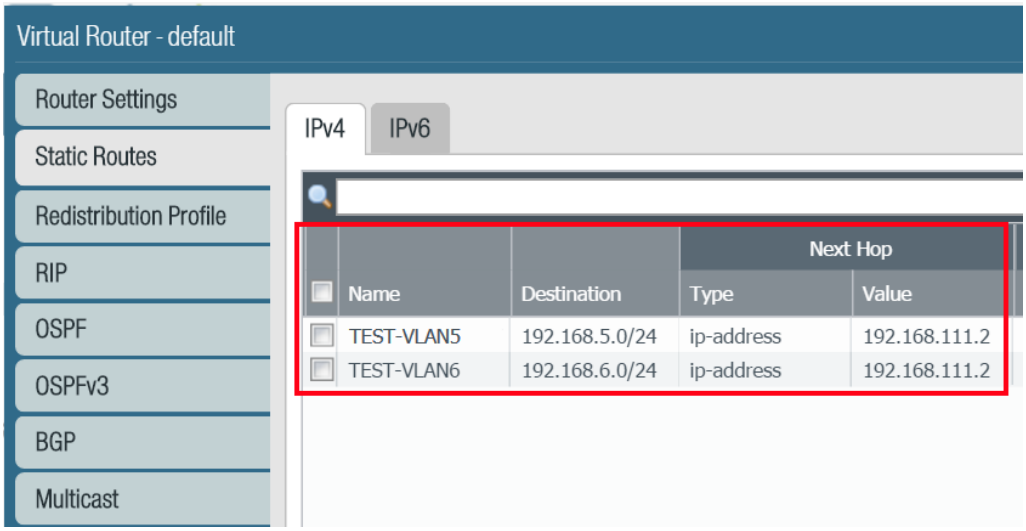
Slika 18: Prikaz nastavitev IP naslovov na požarnem zidu Barracuda F380.



Slika 19: Prikaz nastavitev usmerjanja na požarnem zidu Barracuda F380.



Slika 20: Prikaz nastavitev IP naslovov na požarnem zidu Palo Alto PA-3020.



Slika 21: Prikaz nastavitev usmerjanja na požarnem zidu Palo Alto PA-3020.

```
CP-4600-TEST> set interface bond0.12 ipv4-address 192.168.12.1 subnet-mask 255.255.255.0
CP-4600-TEST> set interface bond0.22 ipv4-address 192.168.22.1 subnet-mask 255.255.255.0
CP-4600-TEST> set interface bond0.112 ipv4-address 192.168.112.1 subnet-mask 255.255.255.0
CP-4600-TEST> set static-route 192.168.5.0/24 nexthop gateway 192.168.112.2 on
CP-4600-TEST> set static-route 192.168.6.0/24 nexthop gateway 192.168.112.2 on
CP-4600-TEST> show  route
Codes: C - Connected, S - Static, R - RIP, B - BGP (D - Default),
       O - OSPF IntraArea (IA - InterArea, E - External, N - NSSA)
       A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed,
       U - Unreachable, i - Inactive

S         0.0.0.0/0           via 10.9.32.1, eth5, cost 0, age 8120
C         10.9.0.0/16         is directly connected, eth5
C         127.0.0.0/8         is directly connected, lo
S         192.168.5.0/24      via 192.168.112.2, bond0.112, cost 0, age 8120
S         192.168.6.0/24      via 192.168.112.2, bond0.112, cost 0, age 8120
C         192.168.12.0/24     is directly connected, bond0.12
C         192.168.22.0/24     is directly connected, bond0.22
C         192.168.112.0/24    is directly connected, bond0.112
```

Slika 22:: Prikaz nastavitev IP naslovov in usmerjanja preko CLI ukazne vrstice na požarnem zidu Check Point 4600.

Pri vseh testih prepustnosti požarnih zidov sta bila izvor prometa generatorja z oznako odjemalec, ki sta simulirala povezovanje uporabnikov na spletni strežnik, preko HTTP protokola. Tudi večina današnjega internetnega prometa poteka ravno preko HTTP protokola.
Odjemalca sta proizvajala promet z naključnimi izvornimi IP naslovi, iz dveh različnih podomrežij: 192.168.1x.0/24, ki smo ga poimenovali podomrežje »Odjemalec 1«. Promet iz tega podomrežja je tekel na strežniško podomrežje 1 - 192.168.5.0/24 do strežnika z IP naslovom 192.168.5.2.
Promet iz podomrežja »Odjemalec 2« z IP naslovi 192.168.2x.0/24 pa se je zaključil na strežniškem podomrežju 2 - 192.168.6.0/24, na strežniku z IP naslovom 192.168.6.2.

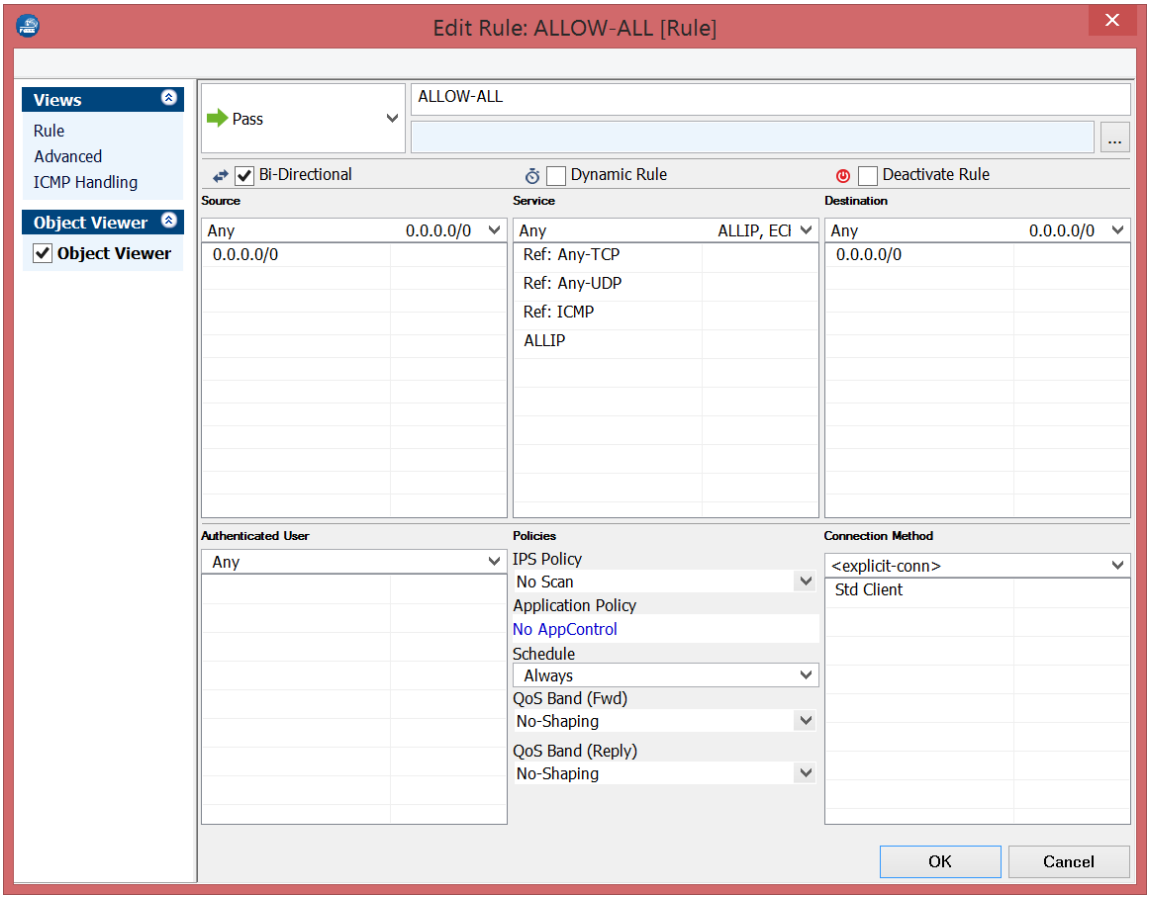
Ta postavitev in konfiguracija požarnih zidov je bila osnova za vse nadaljnje teste.

4.8 Test prepustnosti požarnih zidov brez varnostnih funkcionalnosti

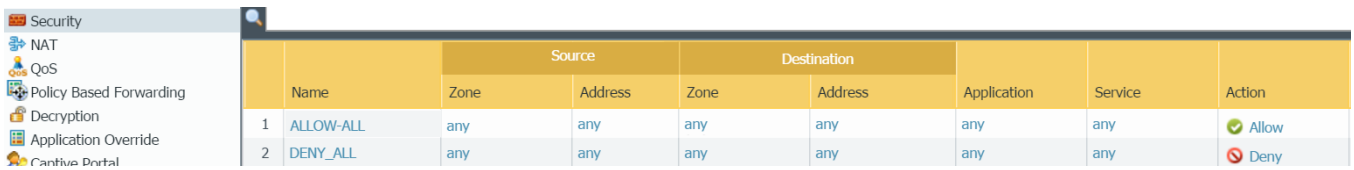
Pri tem testu smo testirali t.i. grobo prepustnost požarnega zidu oz. nazivno prepustnost požarnega zidu, brez vklopa varnostnih funkcionalnosti. Ta podatek proizvajalci navadno podajo kot prvi in najbolj relevanten podatek o zmogljivosti naprave, čeprav se v praksi požarni zid uporablja zgolj zaradi naprednih varnostnih funkcionalnosti, pri uporabi katerih pa se prepustnost zmanjša.

4.8.1 Konfiguracija požarnih zidov

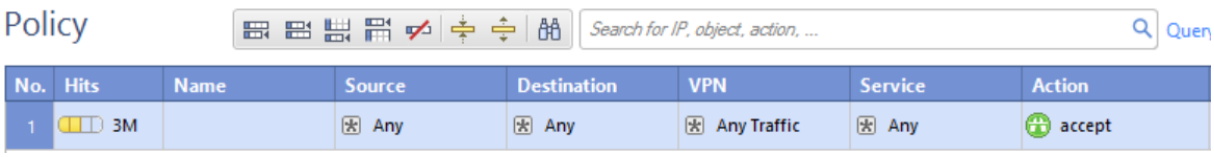
Ker je vseh požarnih zidovih privzeta varnostna politika takšna, da zavrne ves promet, smo morali najprej nastaviti osnovno varnostno pravilo, ki dovoli prehod celotnemu prometu. Politika smo poimenovali »ALLOW-ALL« in je dovoljevala promet iz kateregakoli izvornega IP področja, v katerokoli IP področje.



Slika 23: Prikaz varnostnega pravila »ALLOW-ALL« na požarnem zidu Barracuda F380.



Slika 24: Prikaz varnostnega pravila »ALLOW-ALL« na požarnem zidu Palo Alto PA-3020.



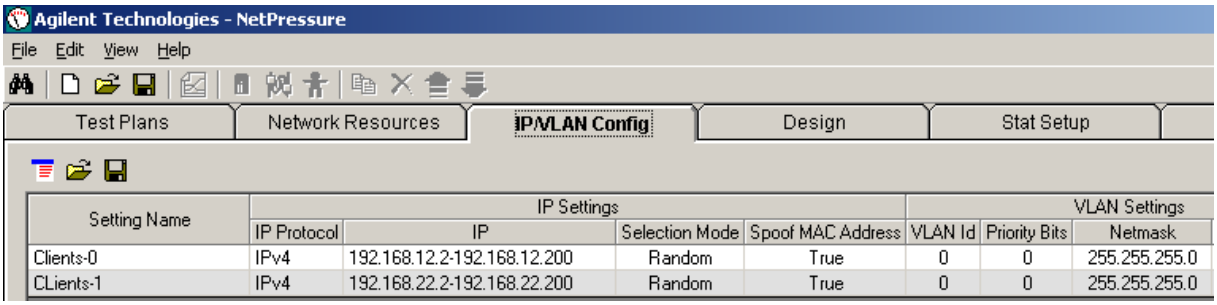
Slika 25:: Prikaz varnostnega pravila »ALLOW-ALL« na požarnem zidu Check Point 4600.

4.8.2 Konfiguracija testerjev

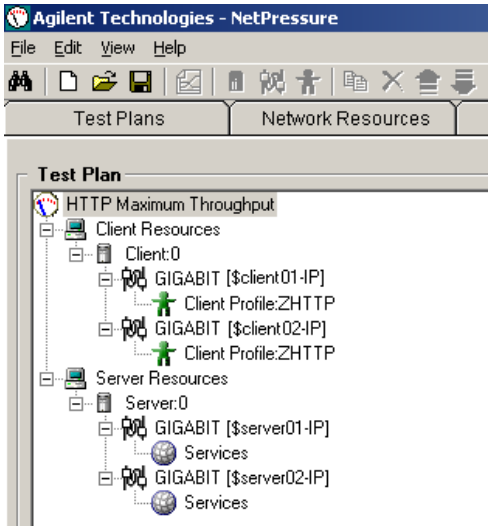
Nato smo pripravili generator omrežnega prometa. Oba generatorja smo nastavili preko »NetPressure« aplikacije, nameščene na prenosnem računalniku za upravljanje. Pred vsakim testom smo morali oba vmesnika na odjemalčevem generatorju prometa prestaviti v ustrezen VLAN glede na požarni zid, na katerem smo izvajali test (1x in 2x). Spremeniti smo morali tudi IP naslov in privzeti prehod odjemalcev ter razpon izvornih IP naslovov za ustvarjanje prometa. VLAN-i, IP naslovi, privzeti prehodi ter razponi IP naslovov pri testu posameznega požarnega zidu so prikazani v spodnji tabeli.

Požarni zid na testu	VLAN		IP naslov	IP naslov privzetega prehoda	razpon izvornih IP naslovov
Barracuda F380	odjemalec 1	10	192.168.10.2	192.168.10.1	192.168.10.2 - 192.168.10.250
	odjemalec 2	20	192.168.20.2	192.168.20.1	192.168.20.2 - 192.168.20.250
Palo Alto PA-3020	odjemalec 1	11	192.168.11.2	192.168.11.1	192.168.11.2 - 192.168.11.250
	odjemalec 2	21	192.168.21.2	192.168.21.1	192.168.21.2 - 192.168.21.250
CheckPoint 4600	odjemalec 1	12	192.168.12.2	192.168.12.1	192.168.12.2 - 192.168.12.250
	odjemalec 2	22	192.168.22.2	192.168.22.1	192.168.22.2 - 192.168.22.250

Tabela 1: VLAN-i, IP naslovi, privzeti prehodi ter razponi IP naslovov pri testu posameznega požarnega zidu.

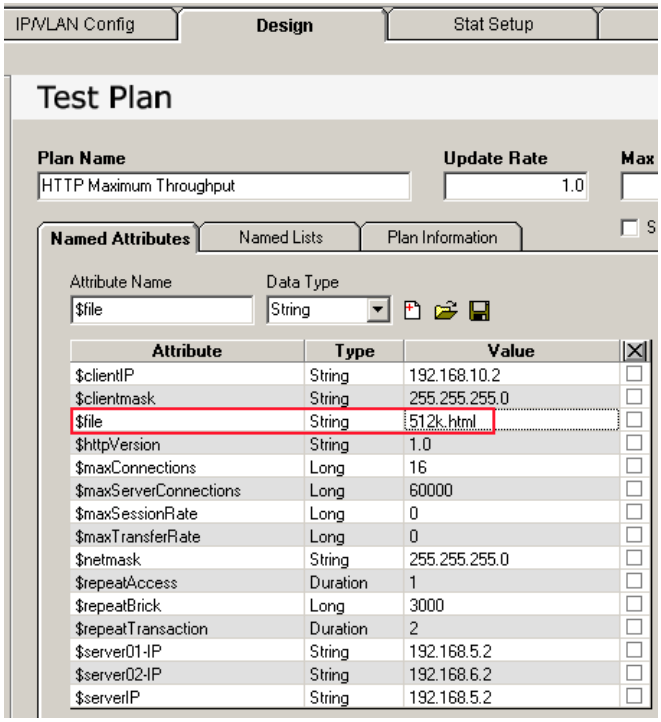


Slika 26: nastavitve IP področij odjemalcev na generatorju omrežnega prometa Agilent N4190B.



Slika 27: nastavitve IP naslovov odjemalcev ter strežnikov na generatorju omrežnega prometa Agilent N4190B

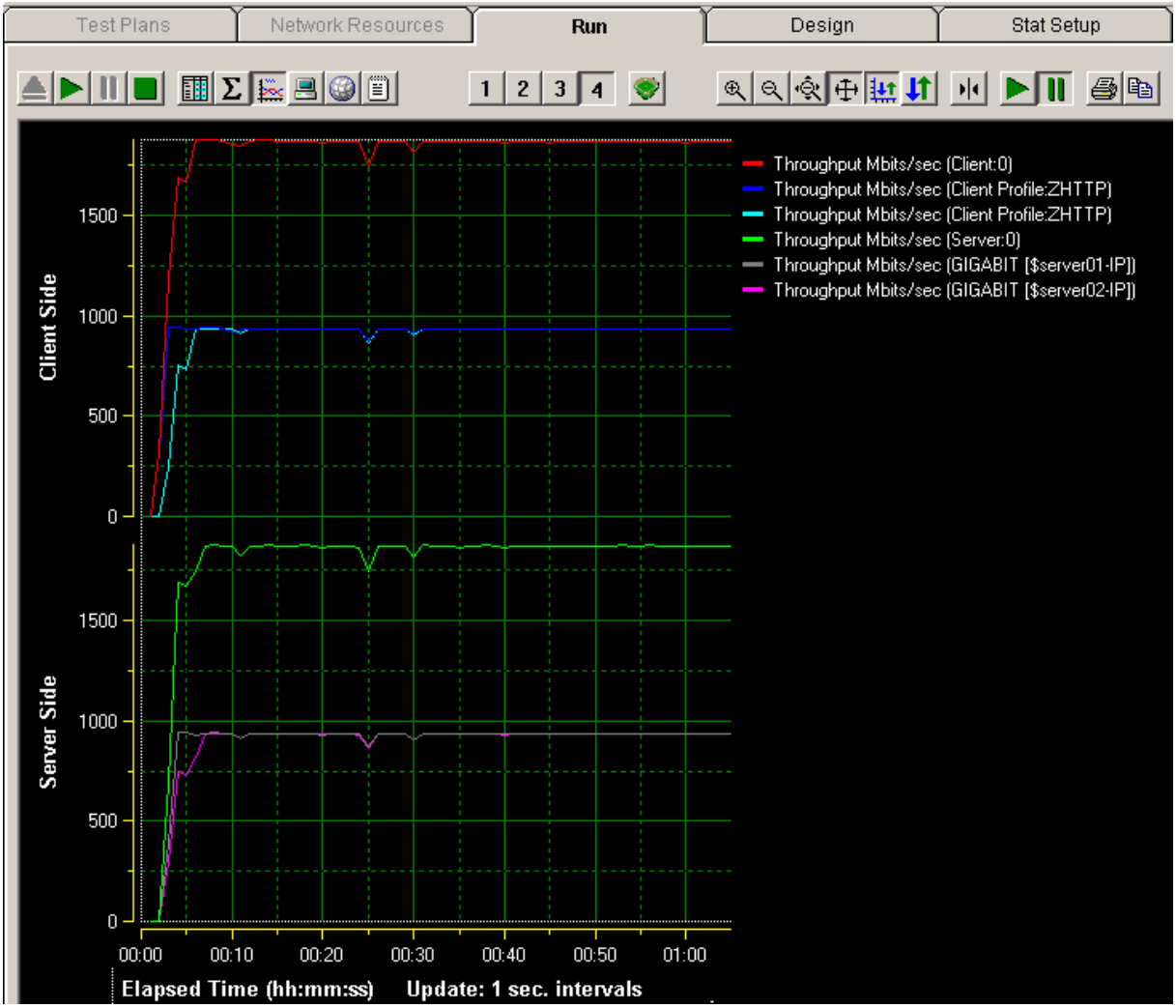
V aplikaciji »NetPressure« smo v delovno okolje naložili v prednastavljeni testni načrt »HTTP Maximum Throughput«, ki se uporablja za testiranje visokih hitrosti prenosa podatkov. Pri tem načrtu odjemalec ustvari veliko količino sej, v katerih iz naključnih izvornih IP naslovih prenaša na strežnik 512KB veliko datoteko, tipa html, preko HTTP protokola.



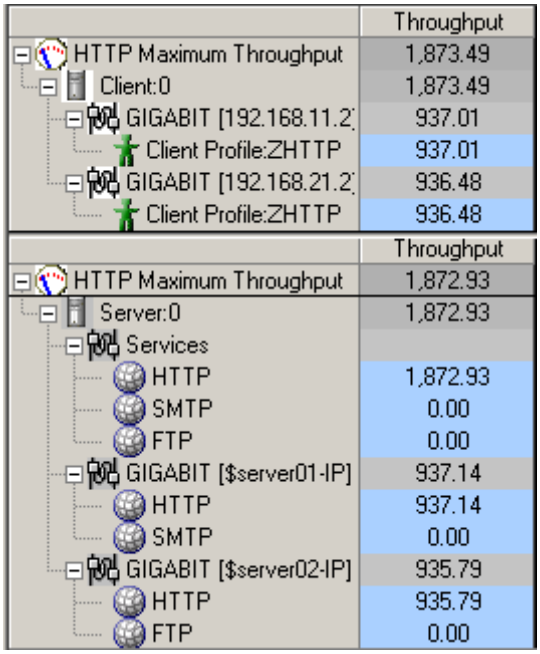
Slika 28: Prikaz nalaganja testnega načrta na generatorja omrežnega prometa preko aplikacije »NetPressure«.

4.8.3 Rezultati testov

Po ustrezni konfiguraciji spremenljivk smo test zagnali in po pretečeni eni minuti shranili rezultate v grafični in tabelarični obliki. Rezultate smo nato vnesli v Excel tabelo in iz podatkov izdelali grafikone.

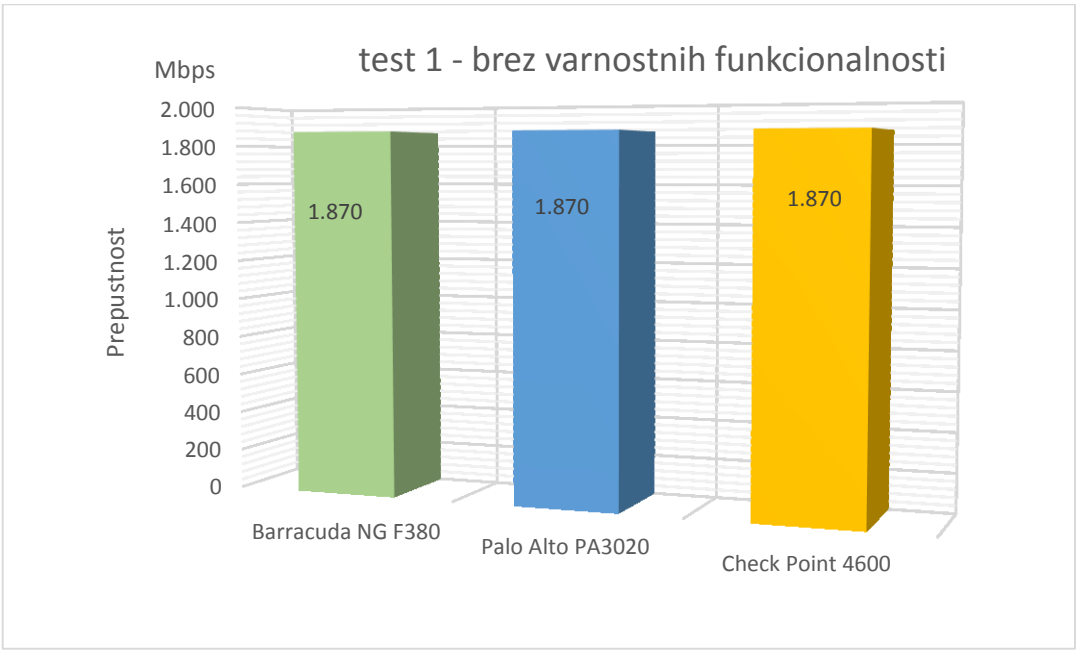


Slika 29: Grafični prikaz prepustnosti požarnega zidu Palo Alto PA-3020 v aplikaciji »NetPressure« pri testu št. 1.



Slika 30:: Statistični prikaz prepustnosti požarnega zidu Palo Alto PA-3020 v aplikacij »NetPressure« pri testu št. 1.

Prepustnost na testu je bila pri vseh treh požarnih zidovih enaka – 1.870 Mbps. Rezultati so pričakovani, saj so nazivne hitrosti, ki jih navajajo proizvajalci, višje od zmogljivosti našega testnega generatorja omrežnega prometa. Dejanska prepustnost se na Ethernet povezavi zaradi izgub raznih protokolov na različnih mrežnih plasteh, ki jim pravimo »overhead«, zmanjša za okoli 6 % [24]. Tako je zgornja meja prepustnosti na 2Gb povezavi 1,88 Gbps, kateri pa smo se zelo približali.



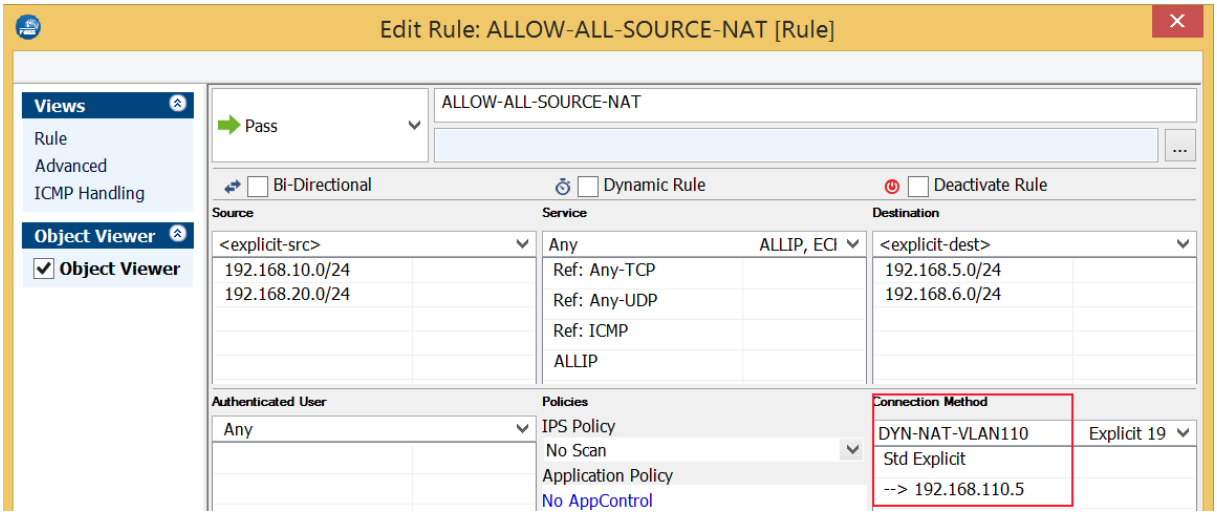
Grafikon 1: Rezultati prepustnosti požarnih zidov na testu št. 1.

4.9 Test prepustnosti pri vklopu NAT funkcionalnosti ter osnovnih varnostnih pravil

Pri tem testu smo testirali prepustnost požarnega zidu ob vklopu NAT funkcionalnosti ter osnovnih varnostnih pravil.
Požarni zid mora pregledati svoja NAT in varnostna pravila zaporedno, dokler promet, ki želi prečkati požarni zid, ne ustreza opisu enega izmed teh. Ko se promet ujame na določeno pravilo, mora požarni zid to pravilo aplicirati. To pa pomeni dodatno porabo procesorske moči ter morebitno zmanjšanje zmogljivosti oz. prepustnosti.

4.9.1 Konfiguracija požarnih zidov

Na požarnih zidovih smo dodali pravila za preslikavo naslovov – NAT. Nastavili smo preslikavo obeh IP področij odjemalcev v IP naslov vmesnika, preko katerega je potekala povezava proti strežniškim IP področjem.
Na spodnji sliki je razvidna nastavitev varnostnega pravila »ALLOW-ALL-SOURCE-NAT« na požarnem zidu Barracuda F380. NAT in varnostno pravilo sta v tem primeru združena v eno pravilo.



Slika 31: Prikaz varnostnega in NAT pravila na požarnem zidu Barracuda F380.

Na požarnih zidovih smo spremenili varnostna pravila tako, da smo pred pravilo »ALLOW-ALL«, ki smo ga nastavili pri prvem testu, vrnili še nekaj pravil, na katere pa se naš testni promet ni ujel. Tako je moral požarni zid pri vsaki na novo vzpostavljeni seji obravnavati vsa pravila od začetka, kar povzroča dodatno obremenitev požarnega zidu.

	Name	Tags	Original Packet			Translated Packet	
			Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT-RULE	none	192.168.11.0/24 192.168.21.0/24	192.168.5.0/24 192.168.6.0/24	any	dynamic-ip-and-port 192.168.111.5	none

Slika 32: Prikaz NAT pravila na požarnem zidu Palo Alto PA-3020.

NAT

No.	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	CLIENT01	SERVER01	Any	WAN-IP-192.168.112.5	Original	Original
2	CLIENT02	SERVER02	Any	WAN-IP-192.168.112.5	Original	Original

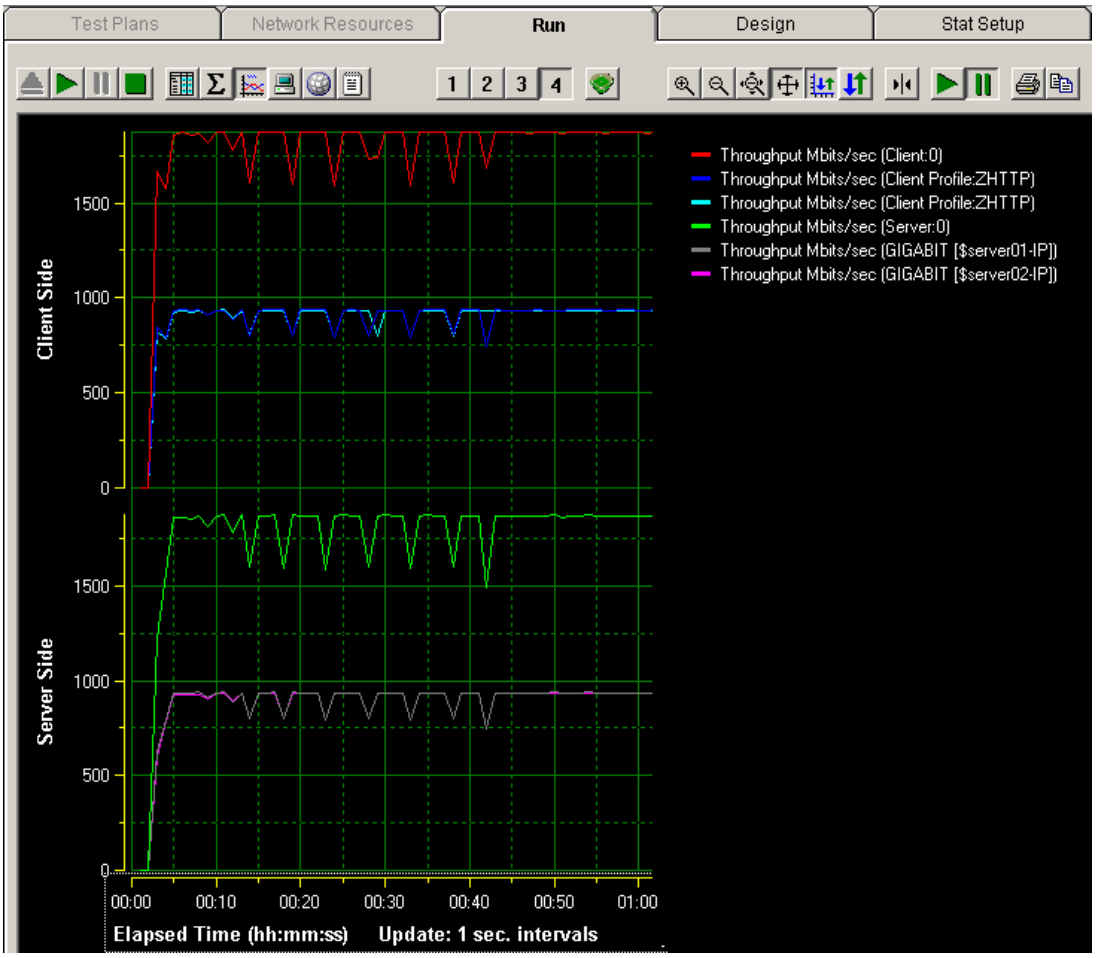
Slika 33: Prikaz NAT pravila na požarnem zidu Check Point 4600.

4.9.2 Konfiguracija testerjev

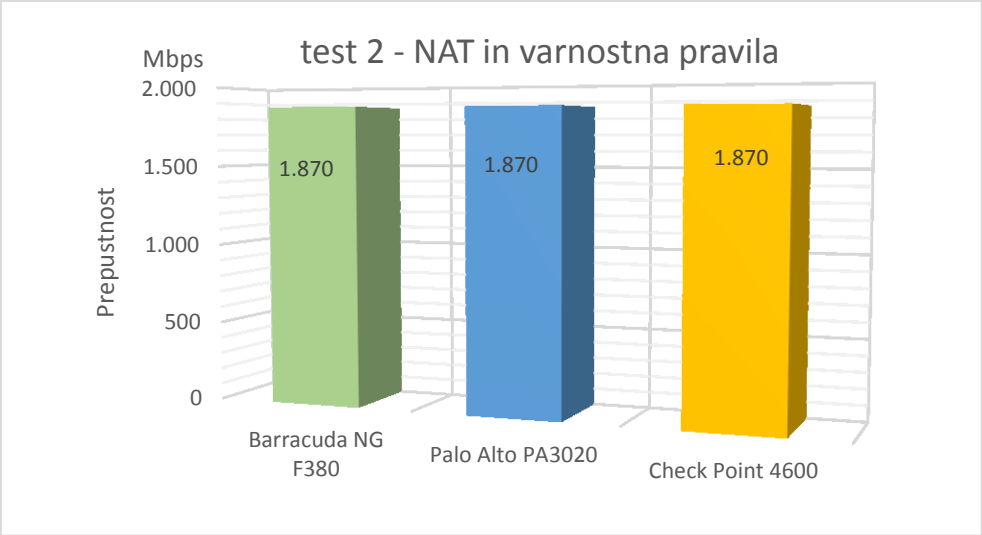
Osnovne konfiguracije testerja nismo spreminjali. Pred testom posameznega požarnega zidu smo spremenili IP nastavitve odjemalcev ter oba vmesnika na odjemalcu prestavili v ustrezen VLAN.

4.9.3 Rezultati testov

Prepustnost je bila tudi pri tem testu pri vseh treh požarnih zidovih enaka – 1.870 Mbps. Dodatne varnostne politike in vklop NAT funkcije torej niso vplivali na zmogljivosti požarnih zidov.



Slika 34: Grafični prikaz prepustnosti požarnega zidu Barracuda F380 pri testu št. 2.



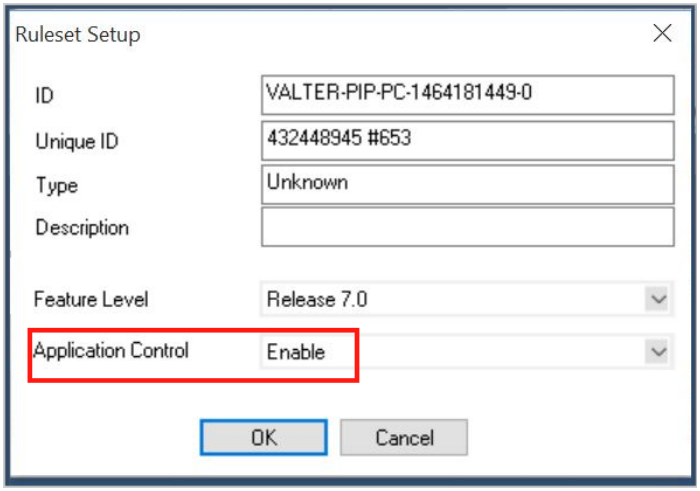
Grafikon 2: Rezultati prepustnosti požarnih zidov na testu št. 2.

4.10 Test prepustnosti pri vklopu funkcionalnosti za razpoznavanje aplikacij

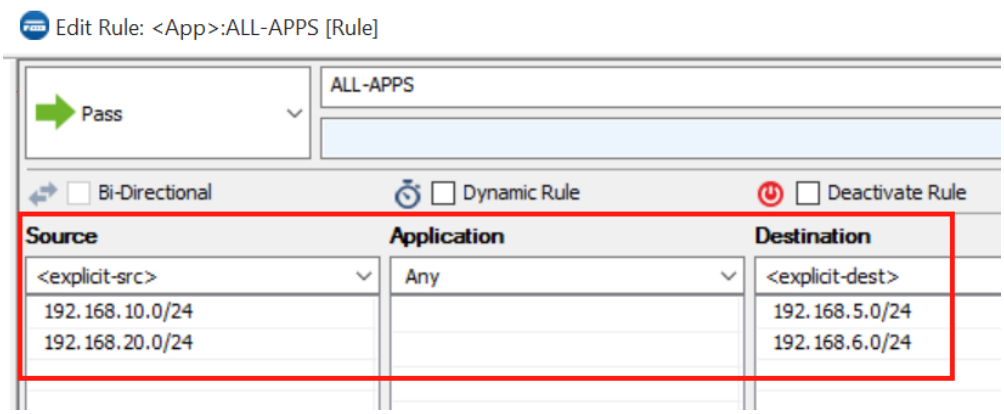
Pri tem testu smo testirali prepustnost požarnega zidu ob vklopu dodatne funkcionalnosti za razpoznavanje aplikacij. Požarni zidovi znajo razpoznati aplikacije in njihovo aktivnost na podlagi podpisa aplikacij in hevristike, vendar na nekaterih požarnih zidovih to predstavlja dodatno obremenitev.

4.10.1 Konfiguracija požarnih zidov

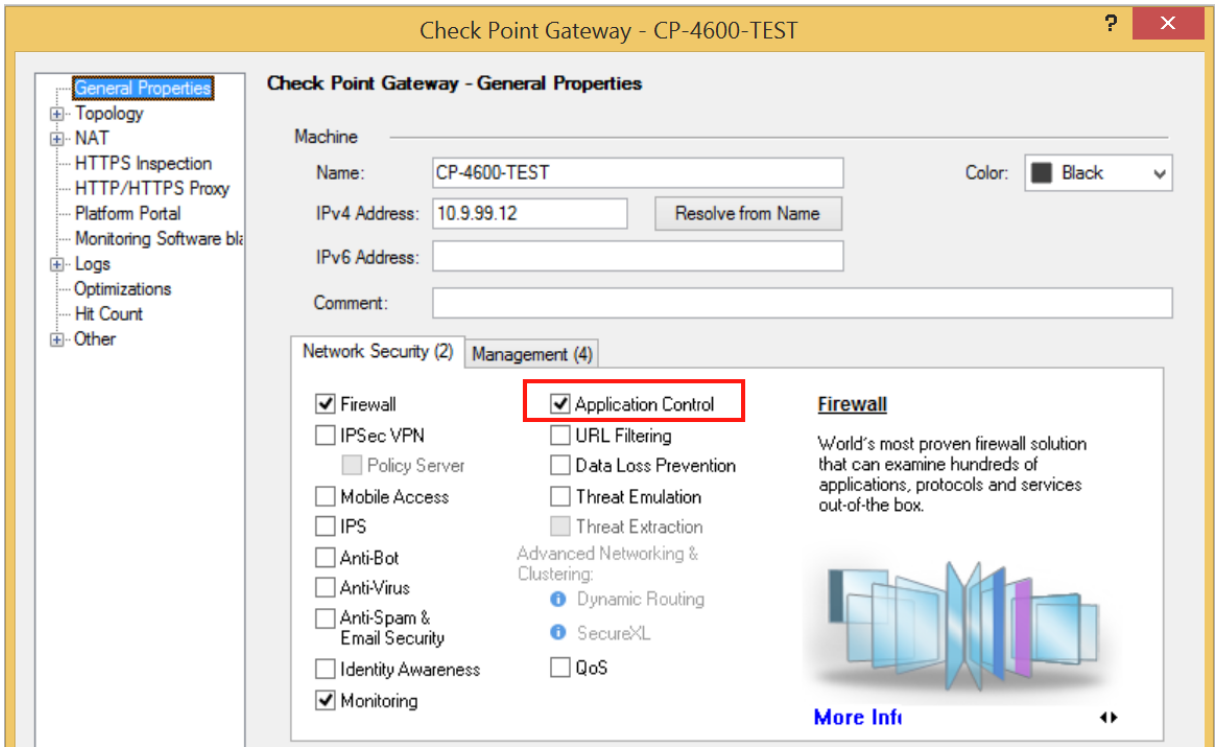
Postopek vklopa razpoznavanja aplikacij se med požarni zidovi razlikuje. Palo Alto PA-3020 požarni zid ima to funkcionalnost vklopljeno že v privzeti nastavitvi in ni nastavljiva. Pri ostalih dveh požarnih zidovih smo morali razpoznavanje aplikacij najprej vklopiti ter nato spremeniti oz. dodati varnostno pravilo z opcijo razpoznavanja aplikacij.



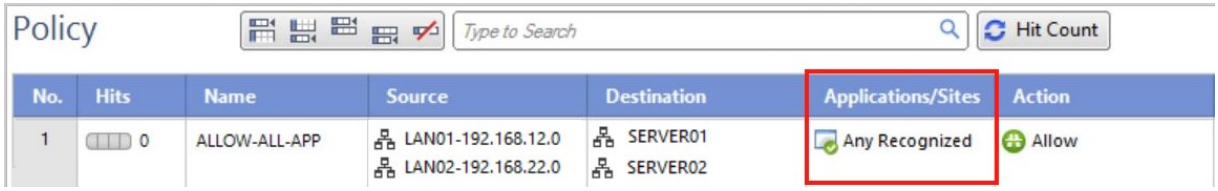
Slika 35: Prikaz vklopa razpoznavanja aplikacij požarnem zidu Barracuda F380.



Slika 36: Prikaz varnostnega pravila z razpoznavanjem aplikacij na požarnem zidu Barracuda F380.



Slika 37: Vklop razpoznavanja aplikacij na požarnem zidu Check Point 4600.



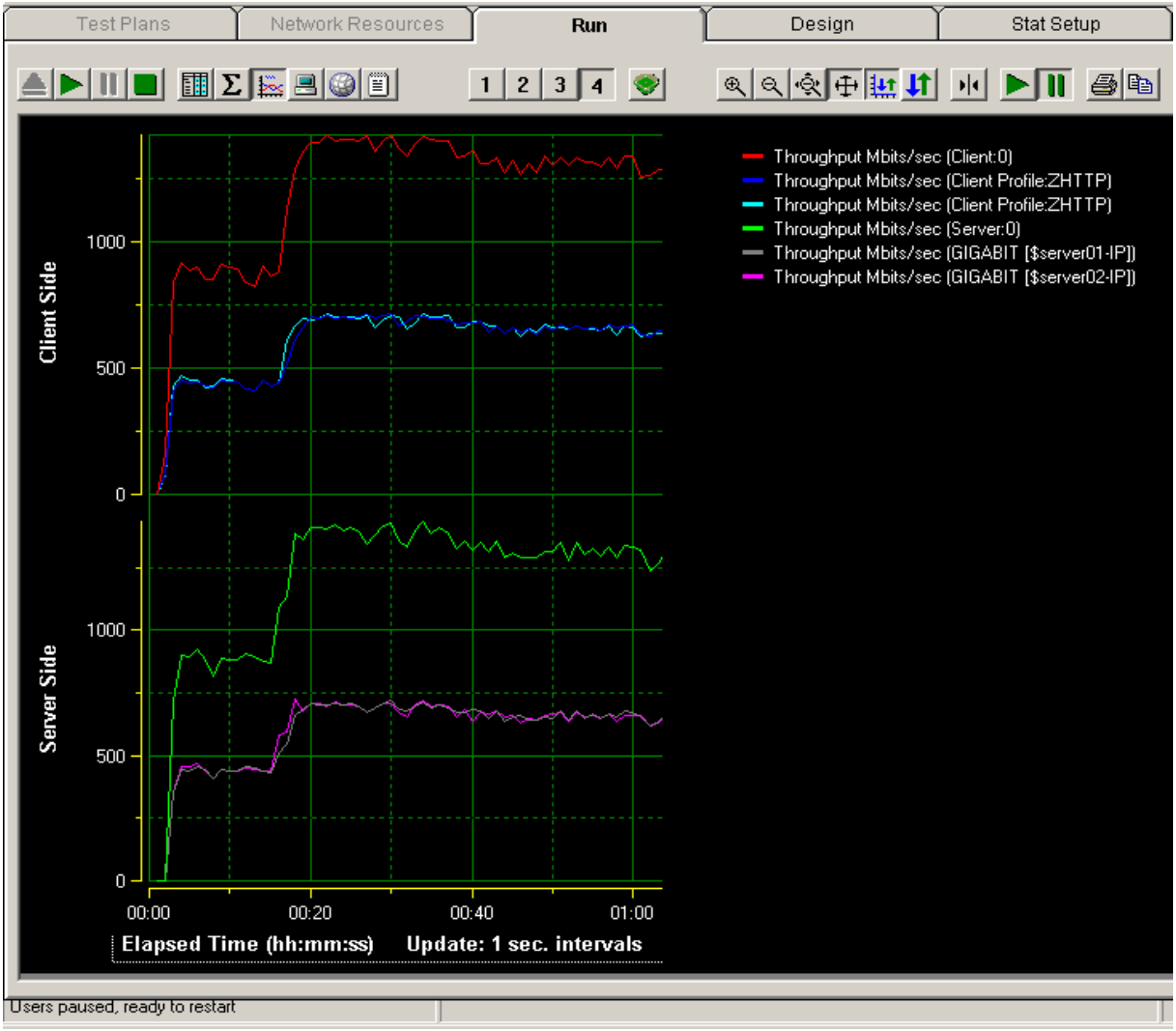
Slika 38: Prikaz varnostnega pravila z razpoznavanjem aplikacij na požarnem zidu Check Point 4600.

4.10.2 Konfiguracija testerjev

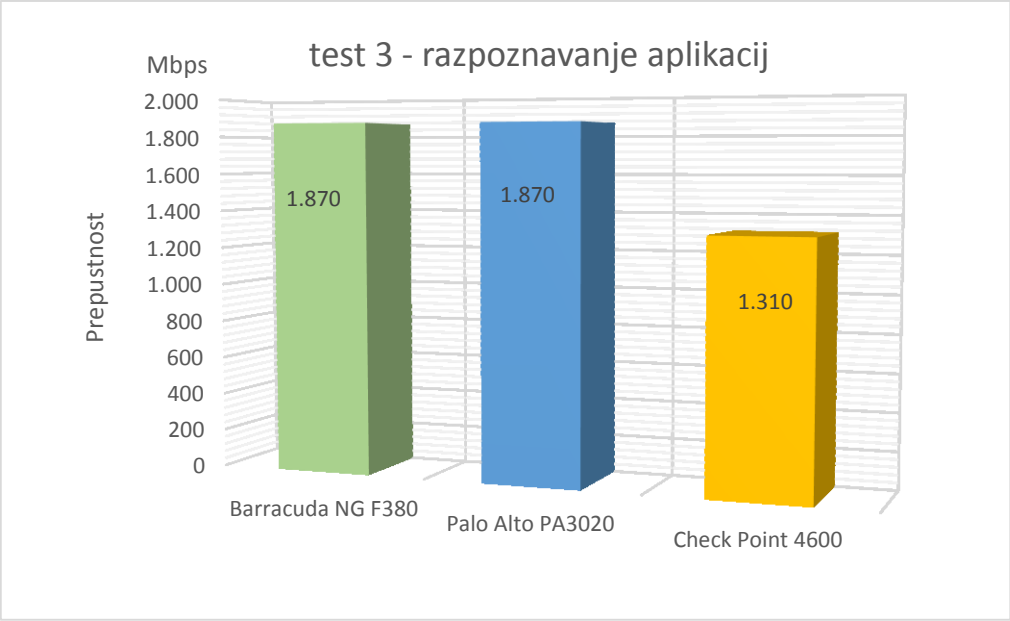
Osnovne konfiguracije testerja nismo spreminjali. Pred testom posameznega požarnega zidu smo spremenili IP nastavitve odjemalcev ter oba vmesnika na odjemalcu prestavili v ustrezen VLAN.

4.10.3 Rezultati testov

Pri tem testu je prišlo do manjših razlik med požarnimi zidovi. Palo Alto PA-3020 je imel to funkcionalnost vklopljeno že pri prejšnjih testiranjih, tako da se rezultat ni spremenil. Barracuda F380 je kljub vklopu dodatne funkcionalnosti ohranila enako prepustnost, pri Check Pointu 4500 pa se je prepustnost zmanjšala.



Slika 39: Grafični prikaz prepustnosti požarnega zidu Check Point 4600 pri testu št. 3.



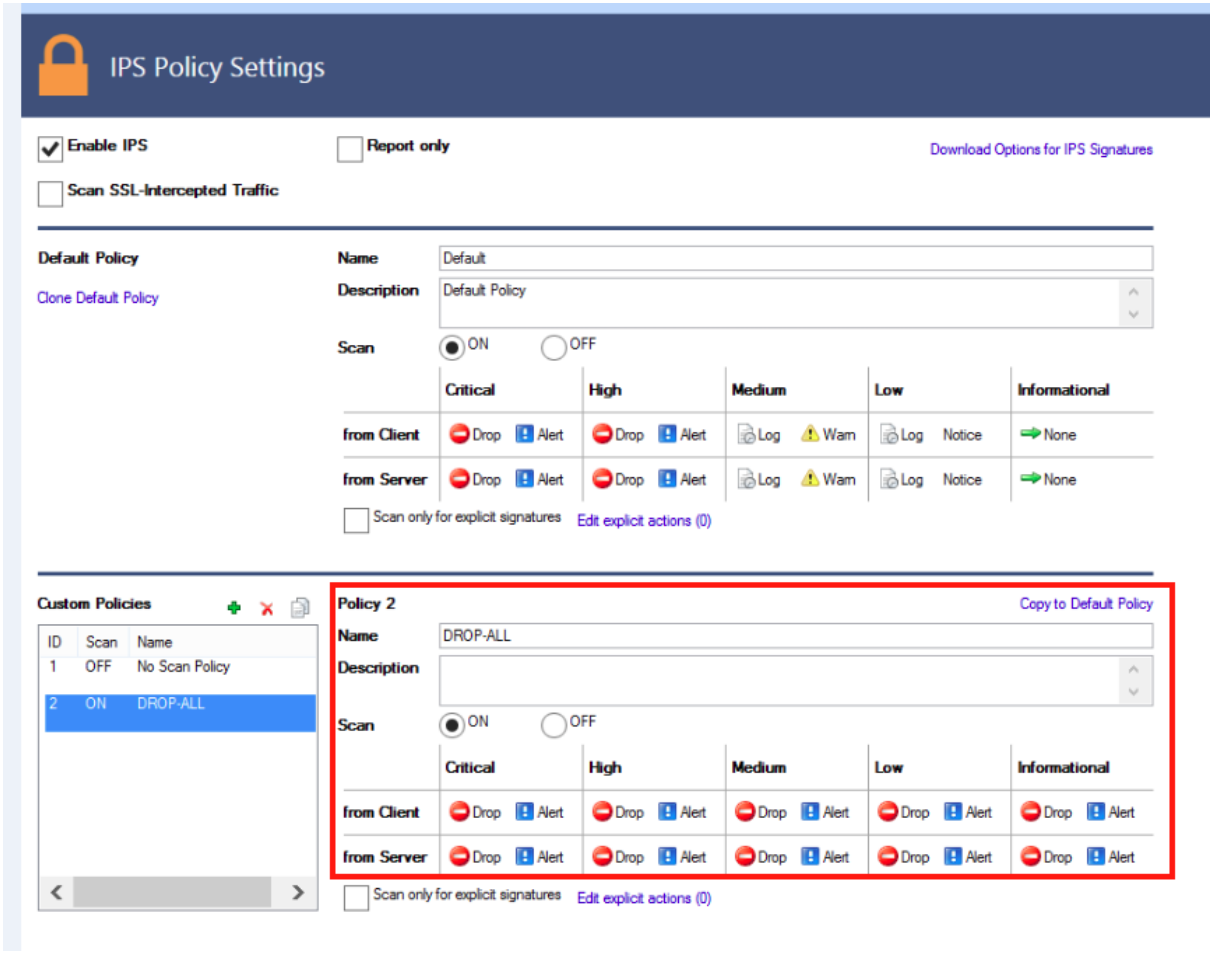
Grafikon 3: Rezultati prepustnosti požarnih zidov na testu št. 3.

4.11 Test prepustnosti pri vklopu funkcionalnosti za preprečevanje groženj

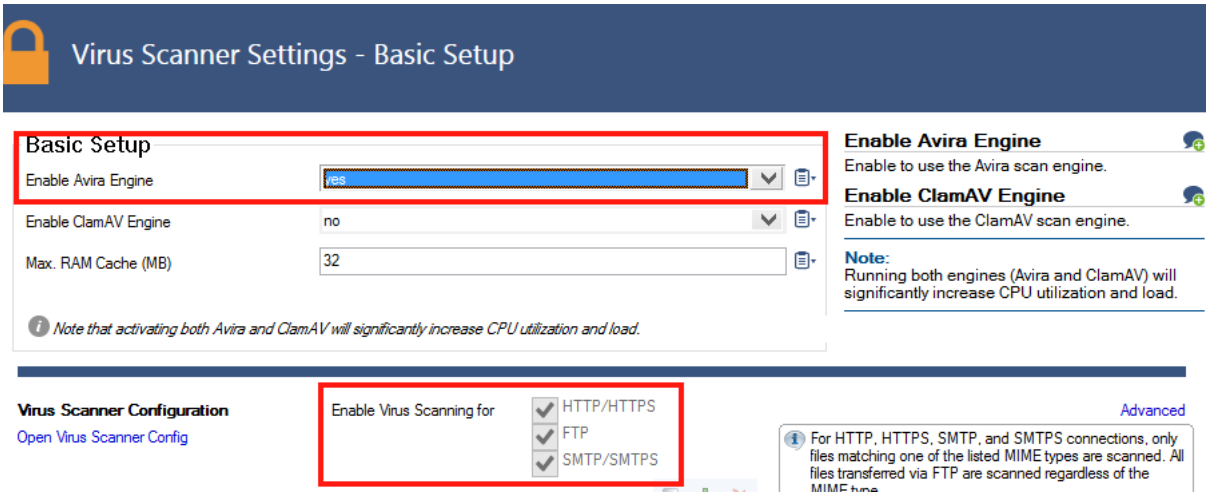
Pri tem testu smo na vklopili najpomembnejše funkcionalnosti na požarnih zidovih – sistem za preprečevanje vdorov, protivirusno zaščito ter zaščito pred zlonamerno programsko kodo. To so tudi najzahtevnejše funkcionalnosti iz vidika procesiranja, zato smo tukaj pričakovali zmanjšanje prepustnosti požarnih zidov.

4.11.1 Konfiguracija požarnih zidov

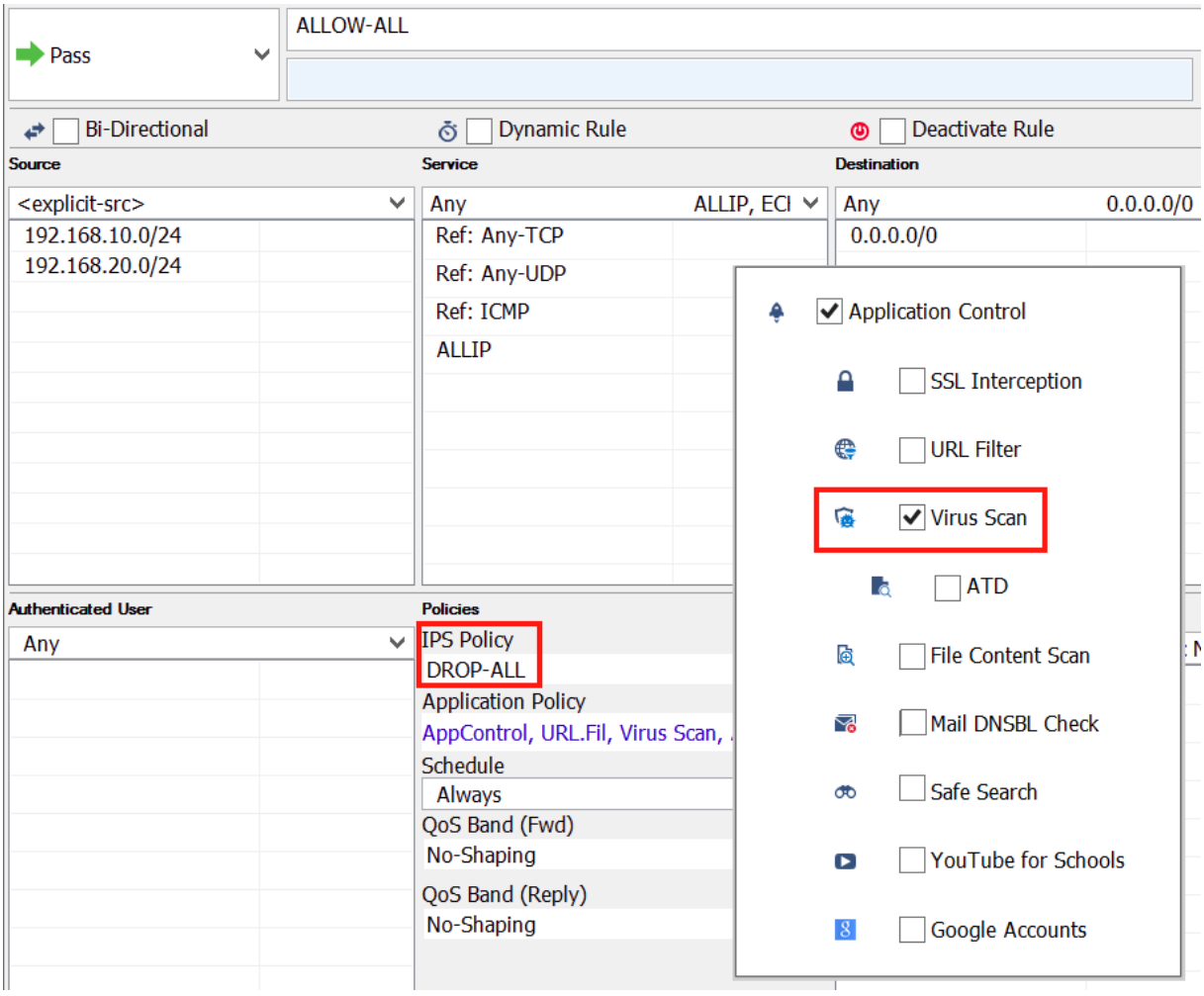
Na požarnem zidu Barracuda F380 smo morali najprej generalno omogočiti IPS funkcionalnost in pripraviti IPS profil. Enako smo storili tudi za protivirusno zaščito. Nato smo v varnostnem pravilu, ki ustreza prometu med odjemalcema in strežnikoma vklopili pripravljen IPS profil ter protivirusno zaščito.



Slika 40: Priprava IPS profila na požarnem zidu Check Point 4600.

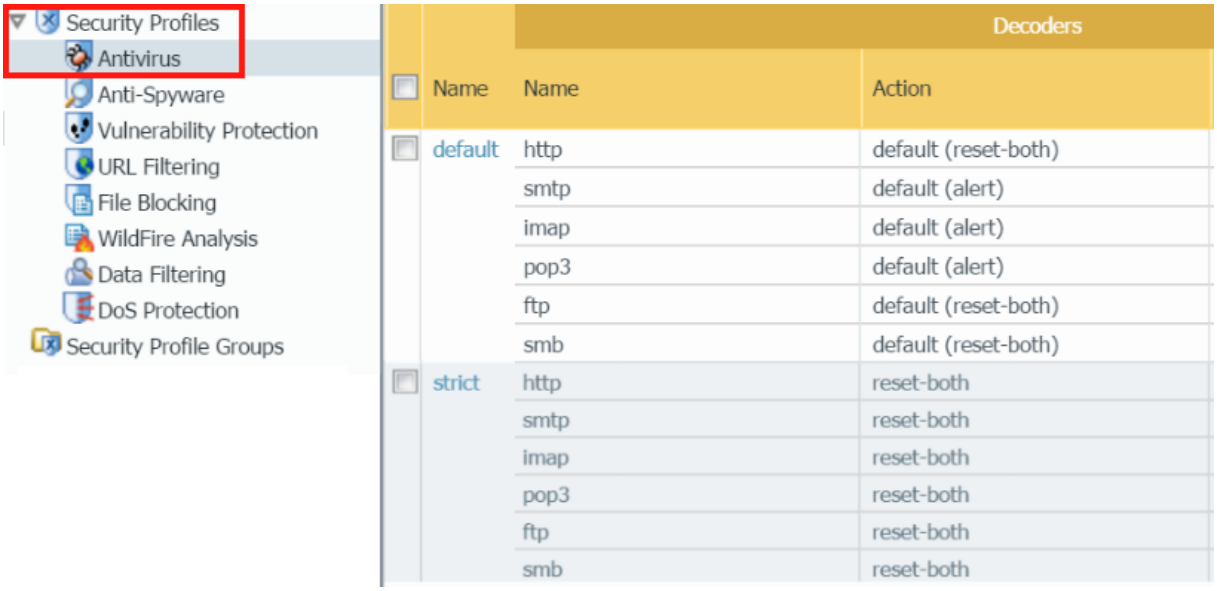


Slika 41: Vklop protivirusne zaščite na požarnem zidu Barracuda F380.



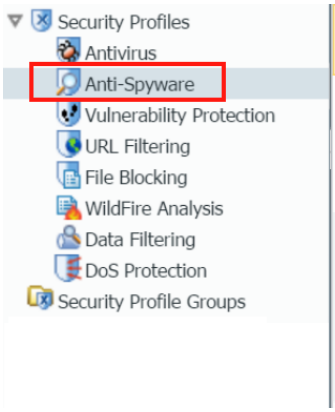
Slika 42: Prikaz nastavitve varnostnega pravila z vklopljeno IPS ter protivirusno zaščito na požarnem zidu Barracuda F380.

Požarni zid Palo Alto ima že v privzeti konfiguraciji pripravljena po dva profila za IPS ter protivirusno zaščito – osnovni »default« profil ter profil s strožjo varnostno politiko »strict«. Poleg teh ima tudi ločen profil za protivohunsko zaščito (ang. AntiSpyware). Vse tri profile lahko izberemo kot opcijo pri konfiguraciji varnostnih pravil. Odločili smo se za strožje profile pri vseh treh opcijah.



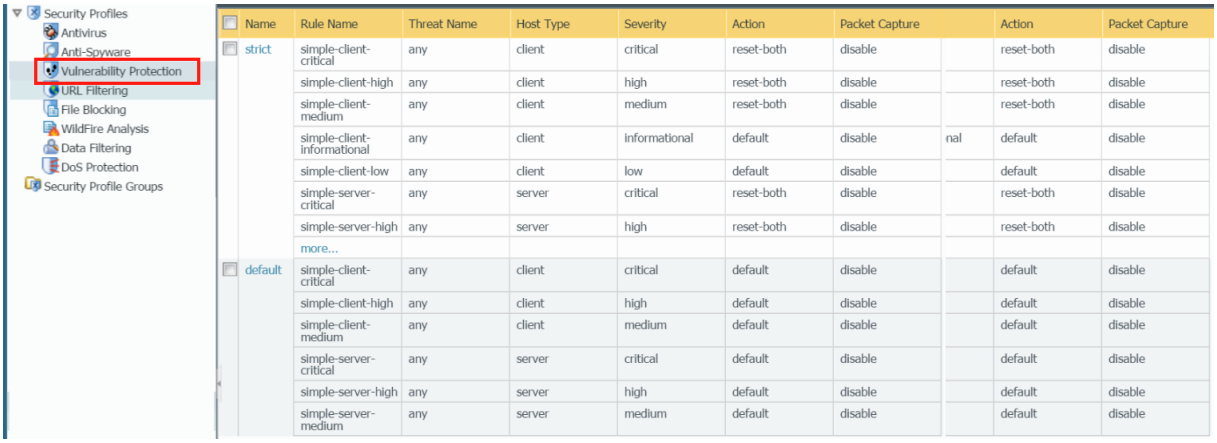
		Decoders	
	Name	Name	Action
	default	http	default (reset-both)
		smtp	default (alert)
		imap	default (alert)
		pop3	default (alert)
		ftp	default (reset-both)
		smb	default (reset-both)
	strict	http	reset-both
		smtp	reset-both
		imap	reset-both
		pop3	reset-both
		ftp	reset-both
		smb	reset-both

Slika 43: Priprava profila za protivirusno zaščito na požarnem zidu Palo Alto PA-3020.



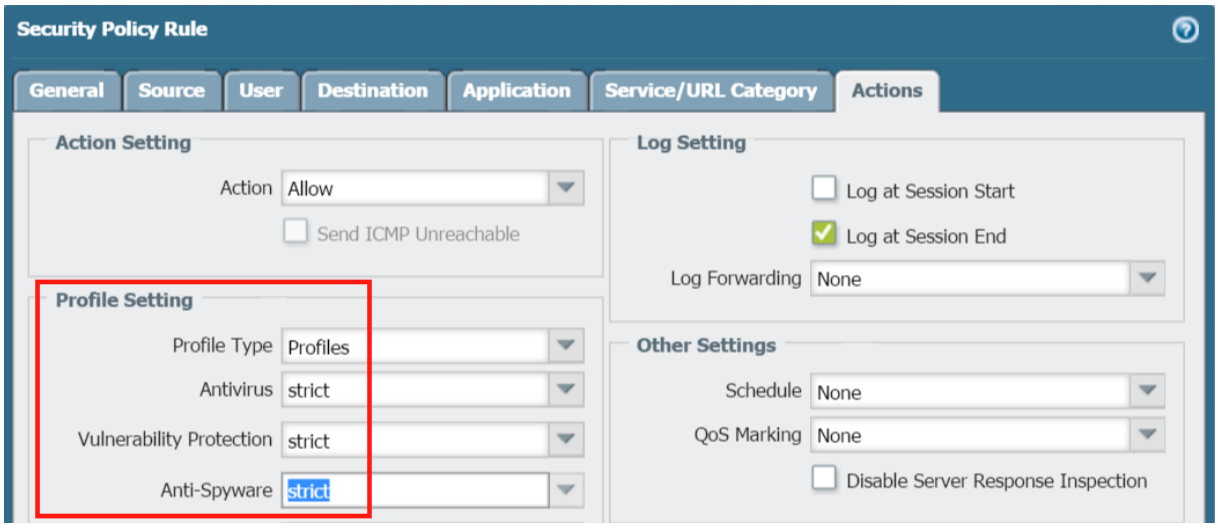
	Name	Rule Name	Threat Name	Severity	Action
	default	simple-critical	any	critical	default
		simple-high	any	high	default
		simple-medium	any	medium	default
		simple-low	any	low	default
	strict	simple-critical	any	critical	reset-both
		simple-high	any	high	reset-both
		simple-medium	any	medium	reset-both
		simple-informational	any	informational	default
		simple-low	any	low	default

Slika 44: Priprava profila za protivohunsko zaščito na požarnem zidu Palo Alto PA-3020.



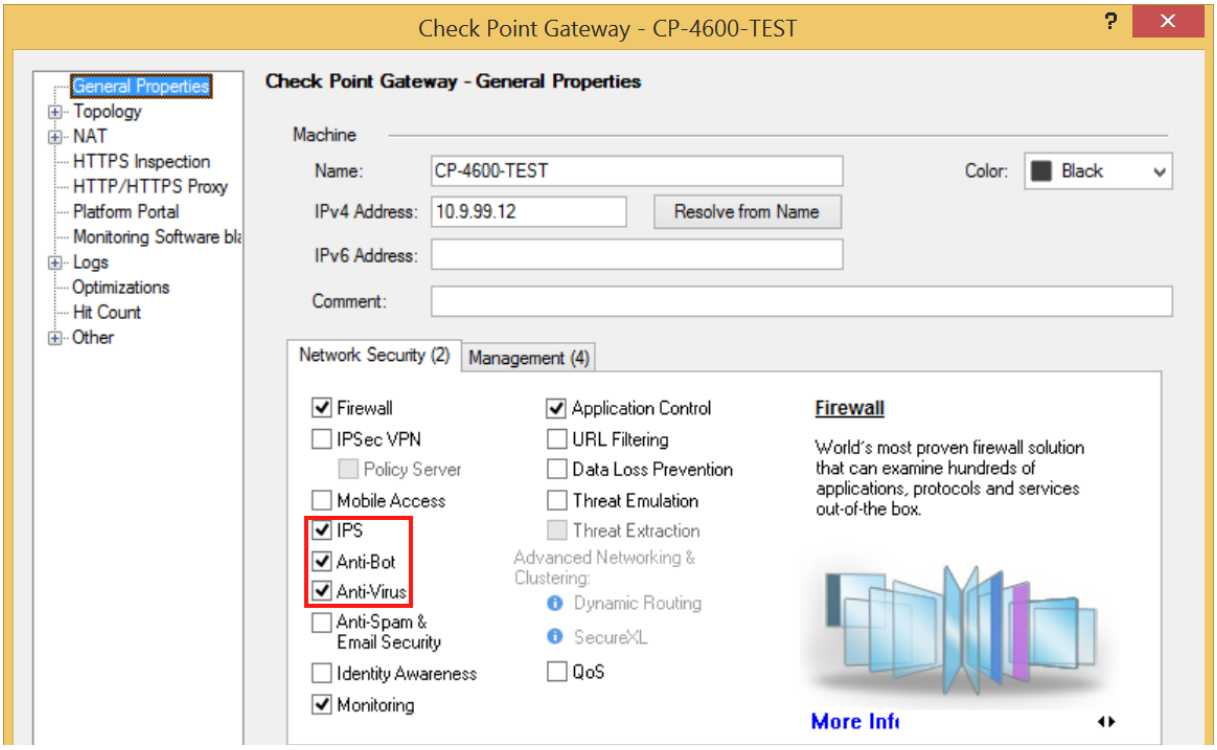
Name	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture		Action	Packet Capture
strict	simple-client-critical	any	client	critical	reset-both	disable		reset-both	disable
	simple-client-high	any	client	high	reset-both	disable		reset-both	disable
	simple-client-medium	any	client	medium	reset-both	disable		reset-both	disable
	simple-client-informational	any	client	informational	default	disable	nal	default	disable
	simple-client-low	any	client	low	default	disable		default	disable
	simple-server-critical	any	server	critical	reset-both	disable		reset-both	disable
	simple-server-high	any	server	high	reset-both	disable		reset-both	disable
	more...								
default	simple-client-critical	any	client	critical	default	disable		default	disable
	simple-client-high	any	client	high	default	disable		default	disable
	simple-client-medium	any	client	medium	default	disable		default	disable
	simple-server-critical	any	server	critical	default	disable		default	disable
	simple-server-high	any	server	high	default	disable		default	disable
	simple-server-medium	any	server	medium	default	disable		default	disable

Slika 45: Priprava IPS profila na požarnem zidu Palo Alto PA-3020.

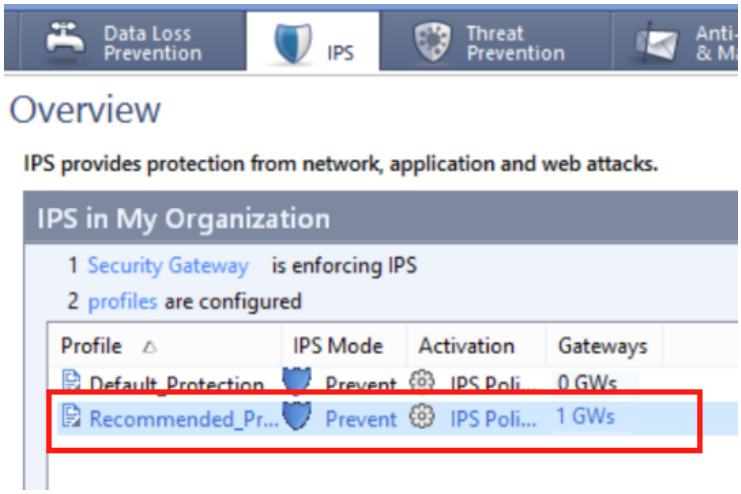


Slika 46: Prikaz nastavitve varnostnega pravila z vklopljeno IPS, protivirusno ter protivohunsko zaščito na požarnem zidu Palo Alto PA-3020.

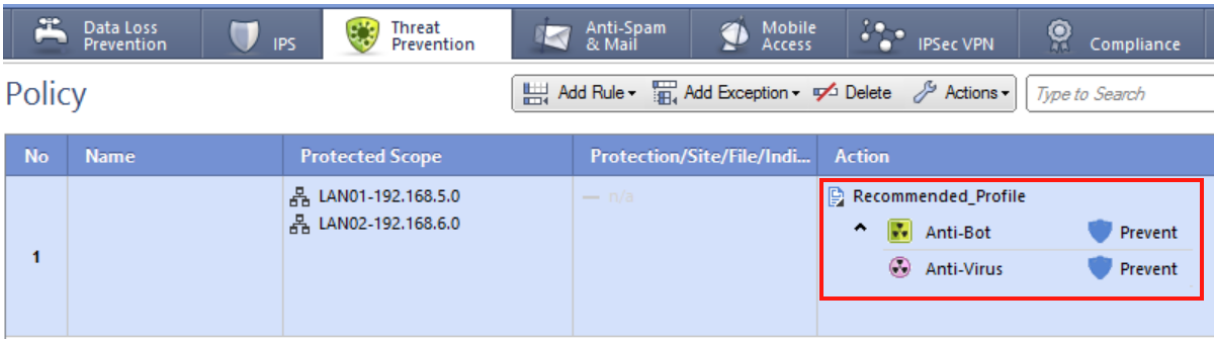
Tudi na požarnem zidu Check Point 4600 smo najprej generalno aktivirali IPS funkcionalnost, protivirusno zaščito ter tudi »Anti-Bot« zaščito. Podobno kot požarni zid Palo Alto ima tudi Check Point v konfiguraciji po dva privzeta profila, osnovni »default« profil ter profil s strožjo varnostno politiko »recommended«. Tudi tukaj smo izbrali in vklopili strožji profil.



Slika 47: Vklop IPS, protivirusne ter »Anti-Bot« zaščite na požarnem zidu Check Point 4600.



Slika 48: Nastavitev IPS zaščite na požarnem zidu Check Point 4600.



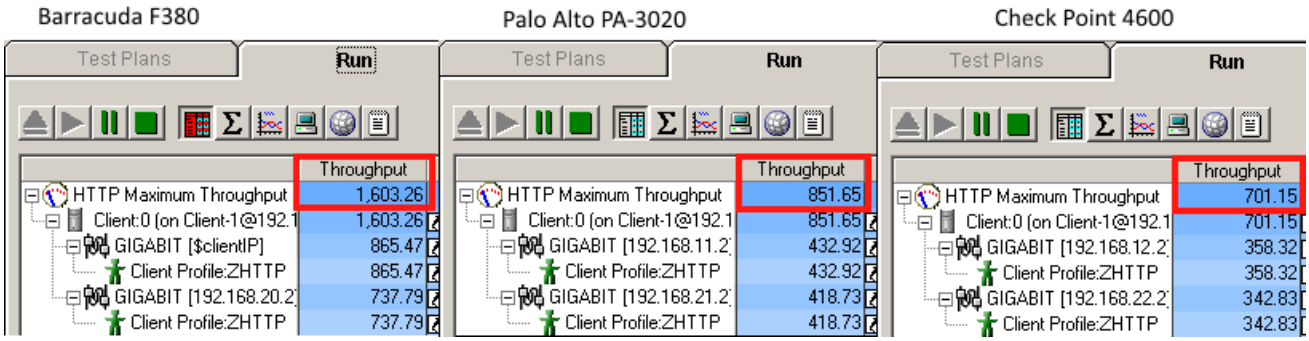
Slika 49: Nastavitev protivirusne ter »Anti-Bot« zaščite na požarnem zidu Check Point 4600.

4.11.2 Konfiguracija testerjev

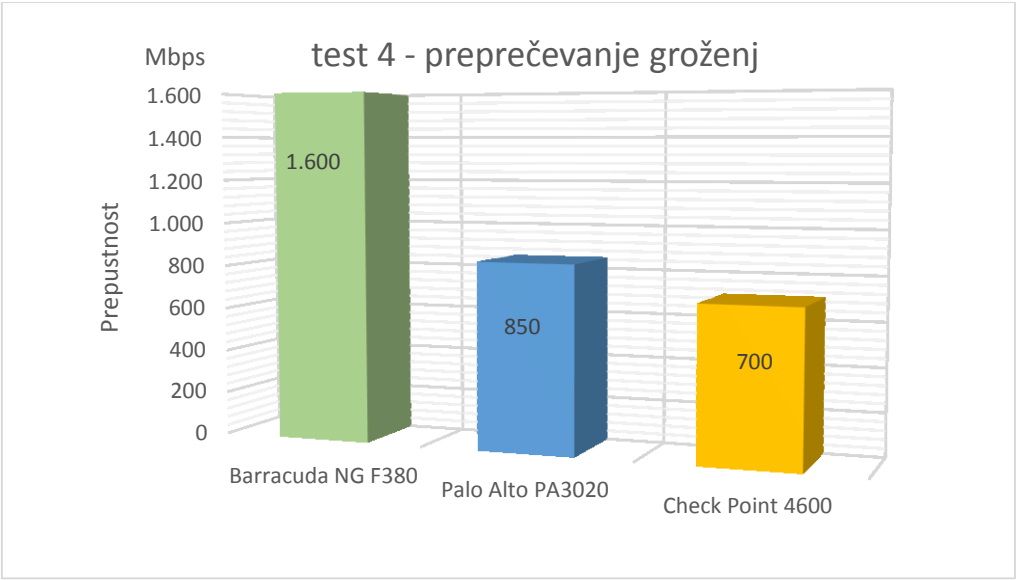
Prepustnost je bila tudi pri tem testu pri vseh treh požarnih zidovih enaka – 1.870 Mbps. Dodatne varnostne politike in vklop NAT funkcije, torej niso vplivali na zmogljivosti požarnih zidov.

4.11.3 Rezultati testov

Pri tem testu je prišlo do velikih razlik med prepustnostjo požarnih zidov. Prepustnost je na dveh požarnih zidovih padla na nazivno raven, ki jo navaja proizvajalec. Pri požarnem zidu Barracuda se je sicer prepustnost tudi znižala, ampak je še vedno ostala krepko nad nazivno ravnjo 1.200 Mbps.



Slika 50: Statistični prikaz prepustnosti požarnih zidov pri testu št. 4.



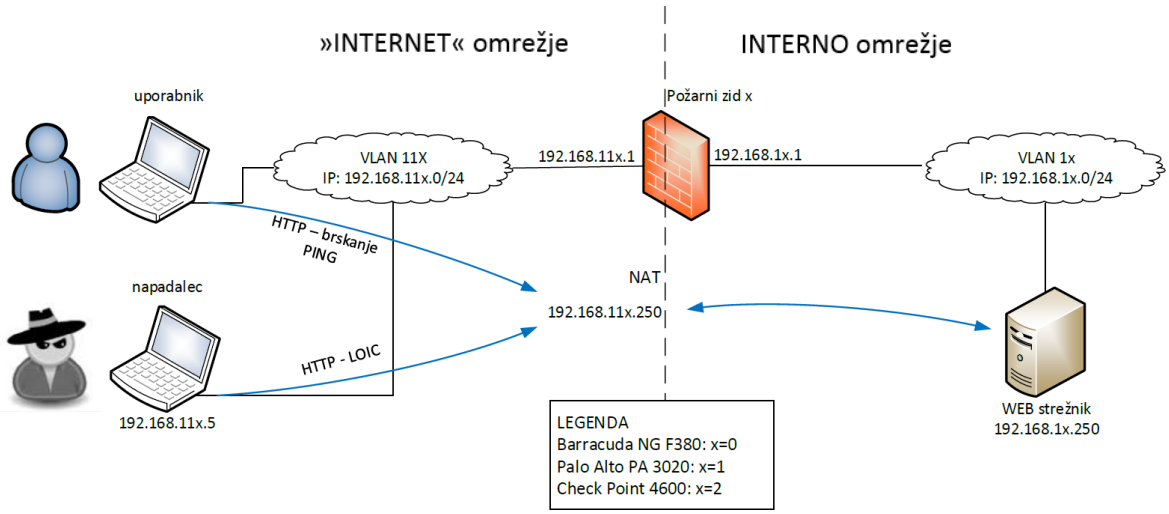
Grafikon 4: Rezultati prepustnosti požarnih zidov na testu št. 4.

4.12 Test učinkovitosti zaščite pred DOS napadi

Test zašite pred DOS napadi smo izvedli tako, da smo na testnem računalniku namestili spletno razvojno okolje za Windows »WampServer« in na njem postavili testno spletno stran. Za testni računalnik smo nato na posameznem požarnem zidu pripravili pravilo za preslikavo naslova spletnega strežnika ter varnostno pravilo, ki dovoljuje promet proti strežniku in tako simulirali objavo v Internet.

V »INTERNET« omrežje smo namestili računalnik, ki je simuliral napadalca. Na njem je tekla znana aplikacija za izvajanje DOS napadov – LOIC. Low Orbit Ion Cannon (LOIC) je odprtokodna aplikacija podjetja Praetox Technologies, napisana v programskem jeziku C#. Prvotno se je uporabljala za izvajanje »stress« testov omrežja, po javni objavi pa sedaj gostuje na več odprtokodnih platformah in se pogosto uporablja za izvajanje DOS napadov. LOIC je orodje za ustvarjanje ogromne količine omrežnega prometa, z namenom izkoriščanja resursov omrežja ali aplikacij. Uporabnik lahko z aplikacijo LOIC sproži DOS napad tako, da poplavi strežnik z nelegitimni TCP, UDP ali HTTP paketi. Takšna visoka obremenjenost omrežja vodi v poslabšanje delovanja in potencialni izpad [25].

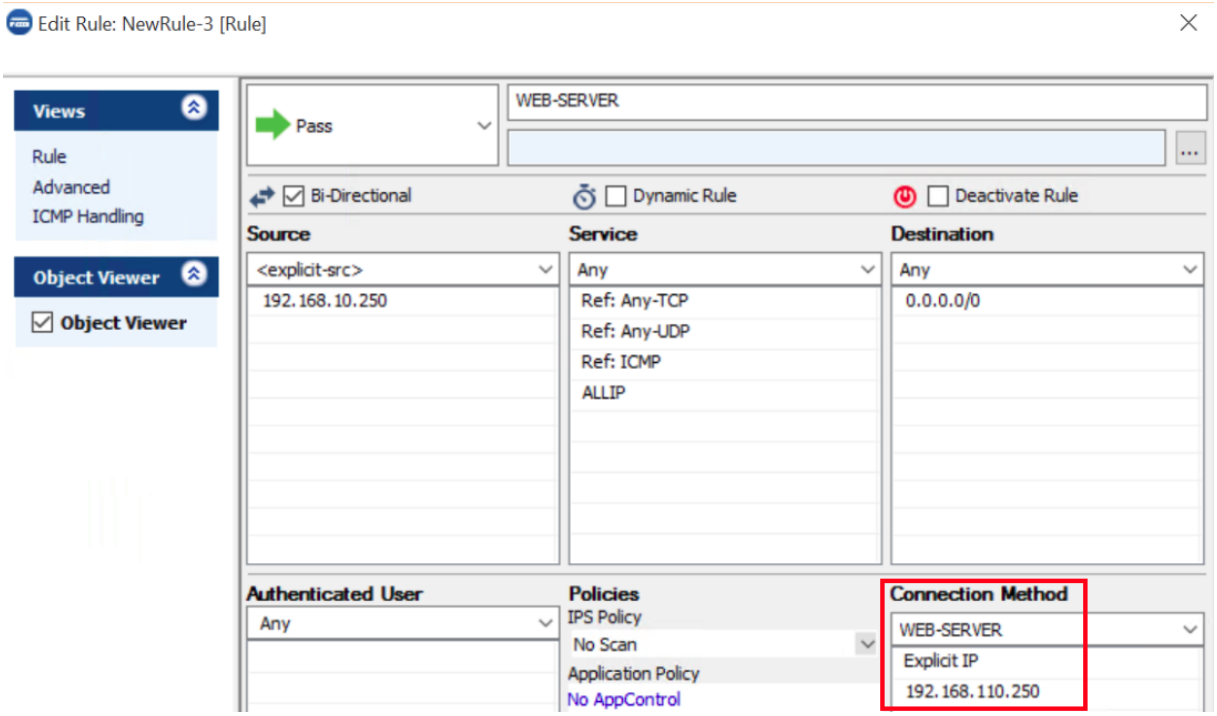
V istem podomrežju se je nahajal tudi kontrolni računalnik, s katerim smo simulirali uporabnika na internetu, ki želi dostopati do testne spletne strani. Poleg brskanja po spletni strani smo proti spletnemu strežniku sprožili še PING in preverjali odzivne čase strežnika, pred in med napadom, ter po aktivaciji varnostnega pravila, za preprečevanje DOS napadov.



Slika 51: Shema testnega okolja pri testu preprečevanja DOS napadov.

4.12.1 Konfiguracija požarnih zidov

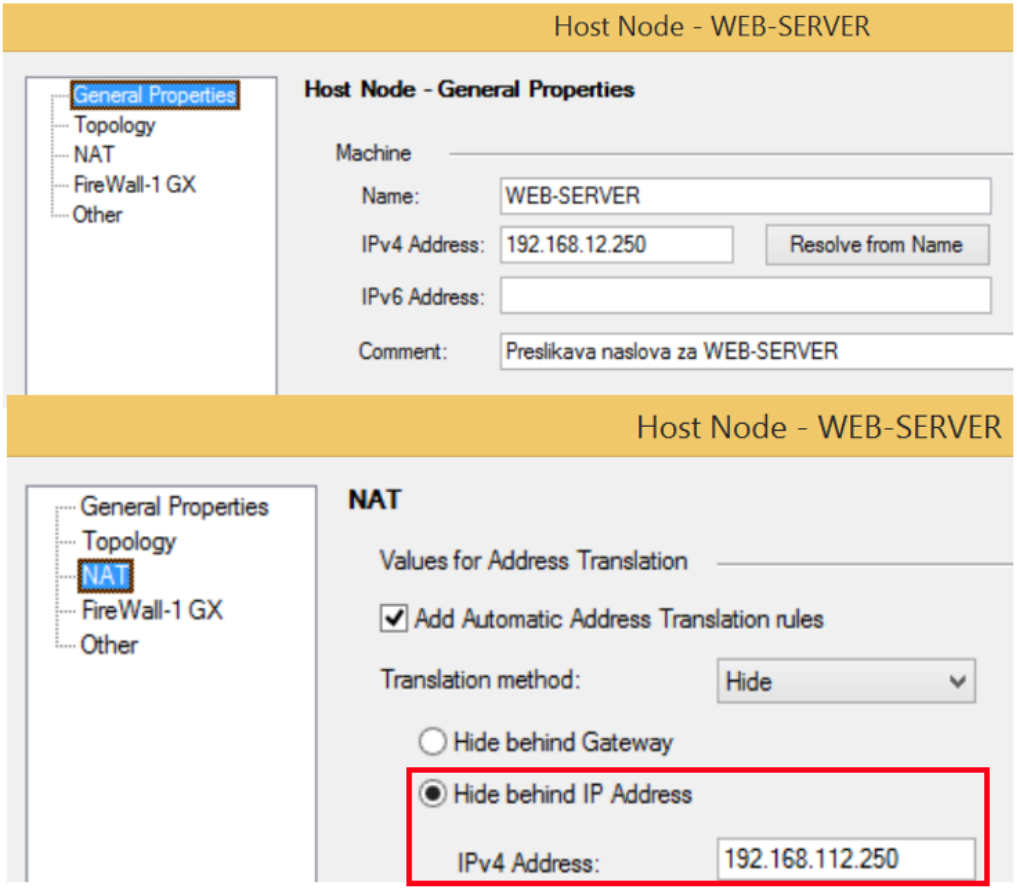
Na požarnih zidovih smo morali naprej objaviti spletni strežnik tako, da lahko do njega dostopajo uporabniki iz »INTERNET« omrežja. To smo naredili s preslikavo naslovov – NAT. Spletni strežnik z IP naslovom 192.168.1x.250 smo preslikali v IP naslov 192.168.11x.250. Poleg tega smo dodali varnostno pravilo, ki dovoljuje promet do spletnega strežnika.



Slika 52: NAT pravilo za spletni strežnik na požarnem zidu Barracuda F380.

	Original Packet						Translated Packet
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation
WEB_SERVER	INSIDE	OUTSIDE	ethernet1/3	192.168.11.250	any	any	static-ip 192.168.111.250 bi-directional: yes

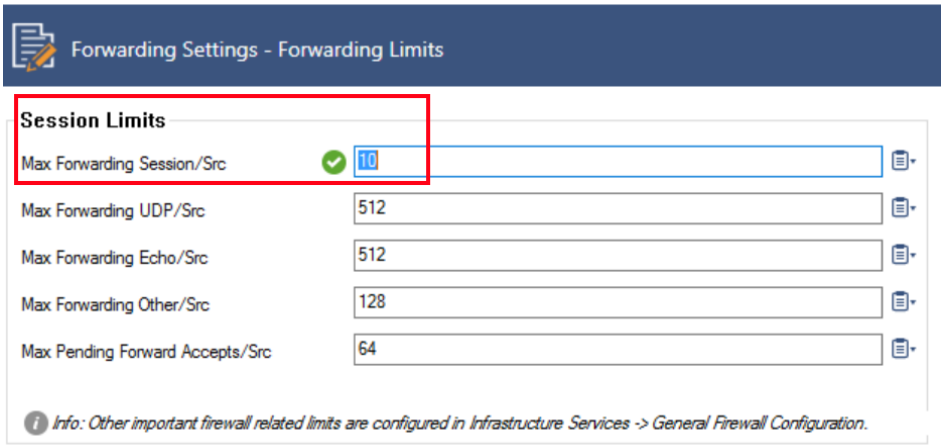
Slika 53: NAT pravilo za spletni strežnik na požarnem zidu Palo Alto PA-3020.



Slika 54: NAT pravilo za spletni strežnik na požarnem zidu Check Point 4600.

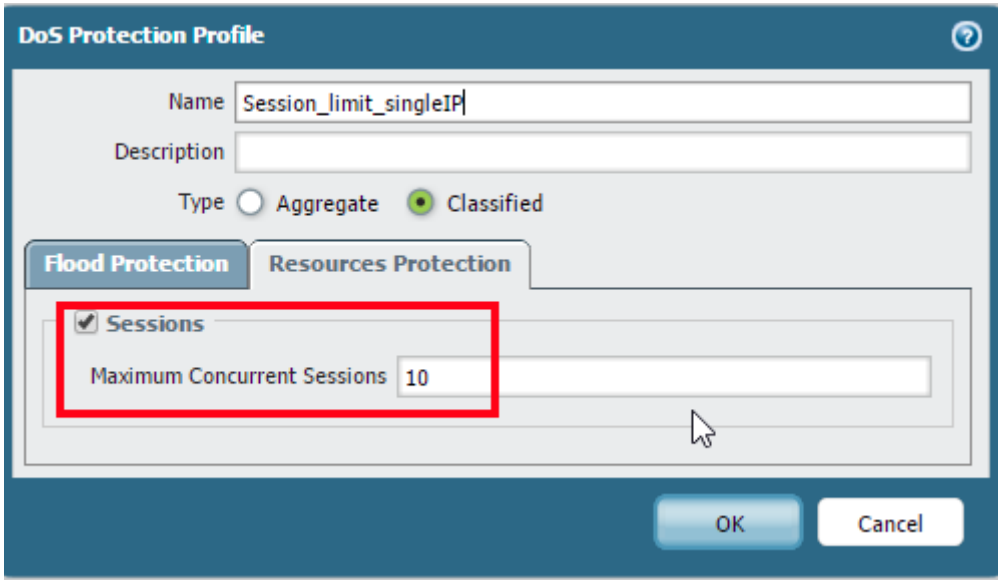
Nato smo na posameznem požarnem zidu pripravili varnostno politiko, ki preprečuje DOS napade. Vsak požarni zid ime več mehanizmov, kako odbiti takšne napade. Odločili smo se za pravilo, ki omeji število sočasnih sej, iz posameznega izvornega IP naslova proti WEB strežniku. Število sej smo omejili na 10.

Na požarnem zidu Barracuda F380 lahko pravilo za omejevanje števila sej vklopimo samo na generalnem nivoju za ves promet, ki prečka požarni zid. Poleg števila TCP sej lahko omejimo še število UDP sej, ECHO oz. ICMP sej ter sej ostalih protokolov.

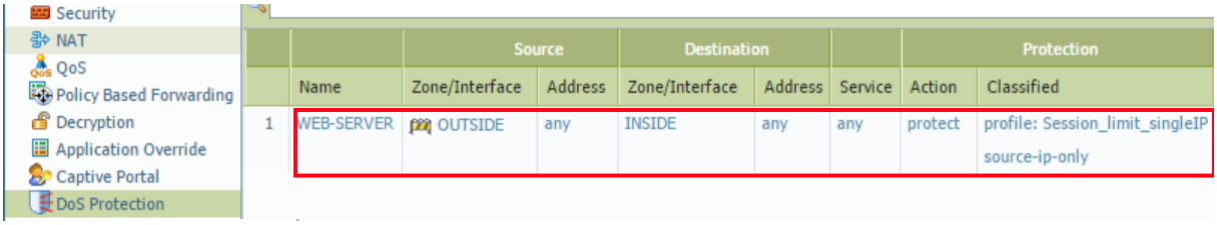


Slika 55: Pravilo za omejevanje števila sej na požarnem zidu Barracuda F380.

Požarni zid Palo Alto ponuja veliko možnosti pri omejevanju DOS napadov. Nastavimo lahko generalna DOS pravila za celoten promet, ki prečka požarni zid, lahko pa DOS pravilo uporabimo na točno določenem prometu glede na izvor/ponor le tega. Pri testu smo najprej pripravili profil za DOS zaščito, kjer smo omejili količino prometa na 10 sej, iz posameznega izvornega IP naslova. Nato smo ta profil uporabili pri varno pravilu za promet iz INTERNET oz. »OUTSIDE« omrežja v INTERNO ali »INSIDE« omrežje.

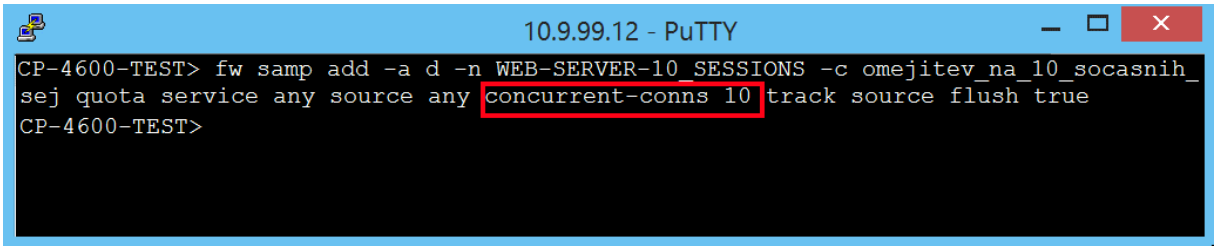


Slika 56: DOS profil na požarnem zidu Palo Alto PA-3020.



Slika 57: Uporaba DOS profila glede na izvor/ponor prometa na požarnem zidu Palo Alto PA-3020.

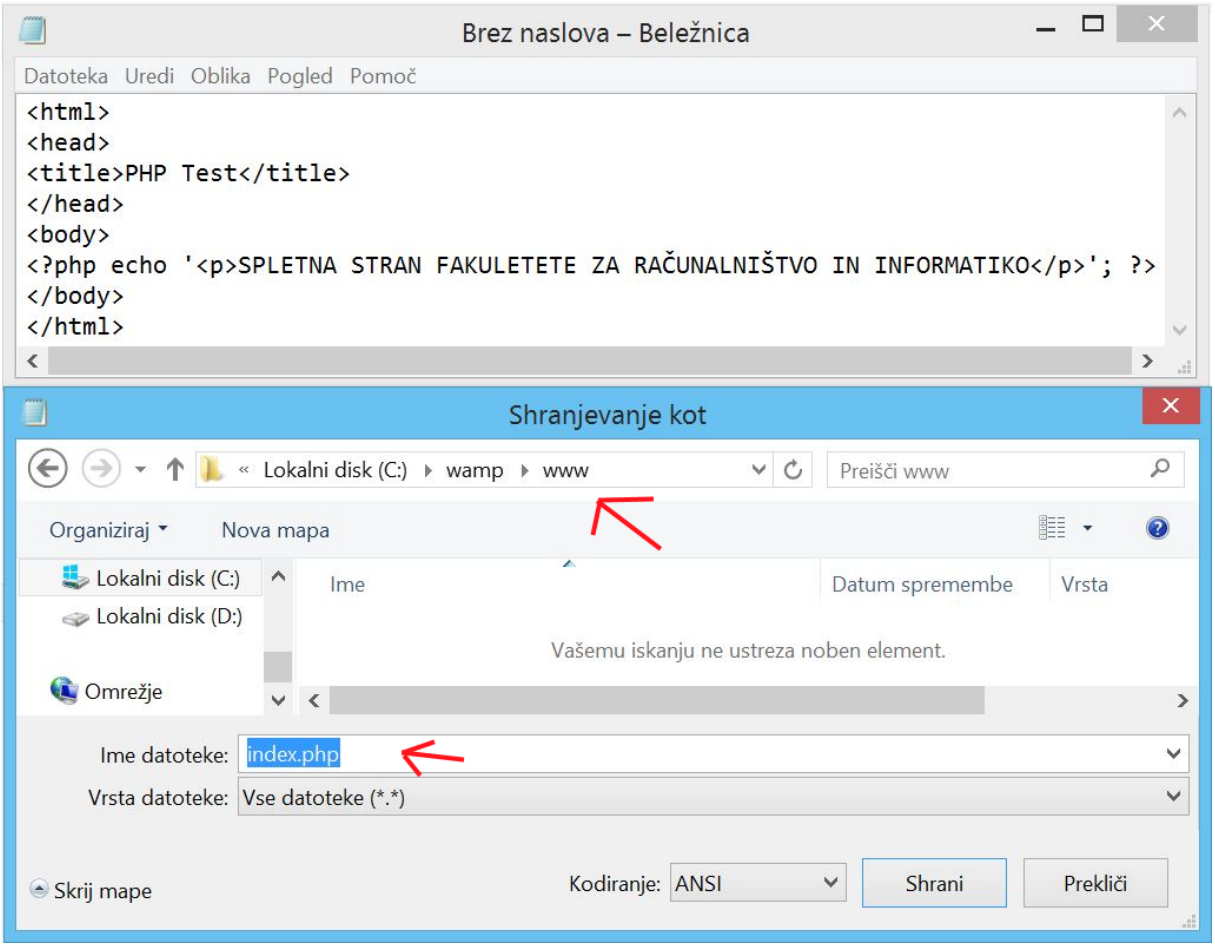
Check Point 4600 ne ponuja konfiguracije omejevanja prometa po številu sej iz aplikacije za upravljanje »SmartDashboard«, ampak moramo omenjeno pravilo namestiti iz CLI ukazne vrstice. Tudi pri Check Point-u lahko pravilo apliciramo na glede na IP ter vrata izvora omrežnega prometa. Uporabili smo ukaz »fw samp«, z nekaj dodatnimi opcijami. »Fw samp« je ukaz, ki se na Check Pointu uporablja pri konfiguraciji protokola, za nadzor sumljivih dejavnosti (Firewall Suspicious Activities Monitoring Protocol). Omejitev števila sej na 10 smo dosegli z opcijo »concurrent-conns 10«.



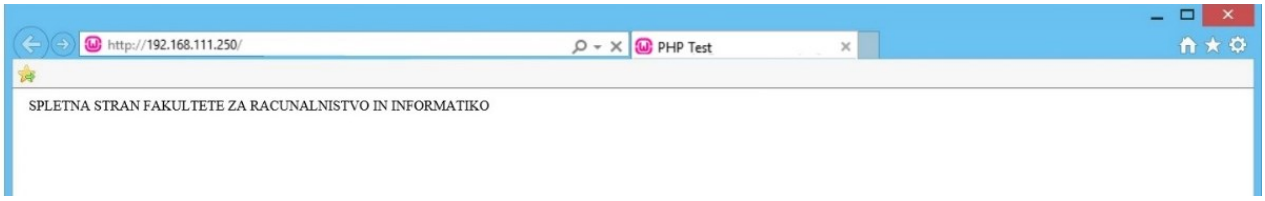
Slika 58: Nastavitev omejevanja števila sej na požarnem zidu Check Point 4600.

4.12.2 Konfiguracija testerjev

Nastavitev WAMP strežnika na testnem računalniku je bila enostavna. Najprej smo program namestili. Nato smo v programu »Beležnica« napisali zelo osnovno spletno stran in jo shranili v »WWW« direktorij programa WAMP. Sledila je samo še objava spletne strani preko gumba »Put Online« in spletna stran je že bila dostopna.

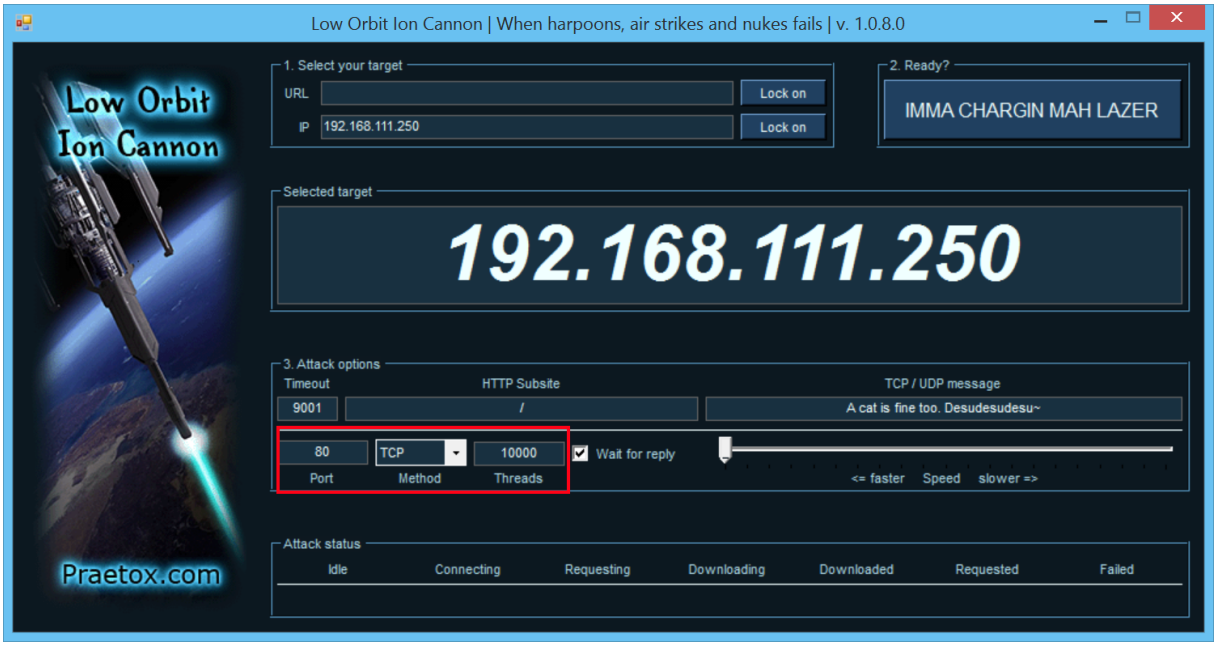


Slika 59: Koda testne spletne strani ter shranjevanje v mapo »wamp\www«.



Slika 60:Prikaz testne spletne strani v brskalniku.

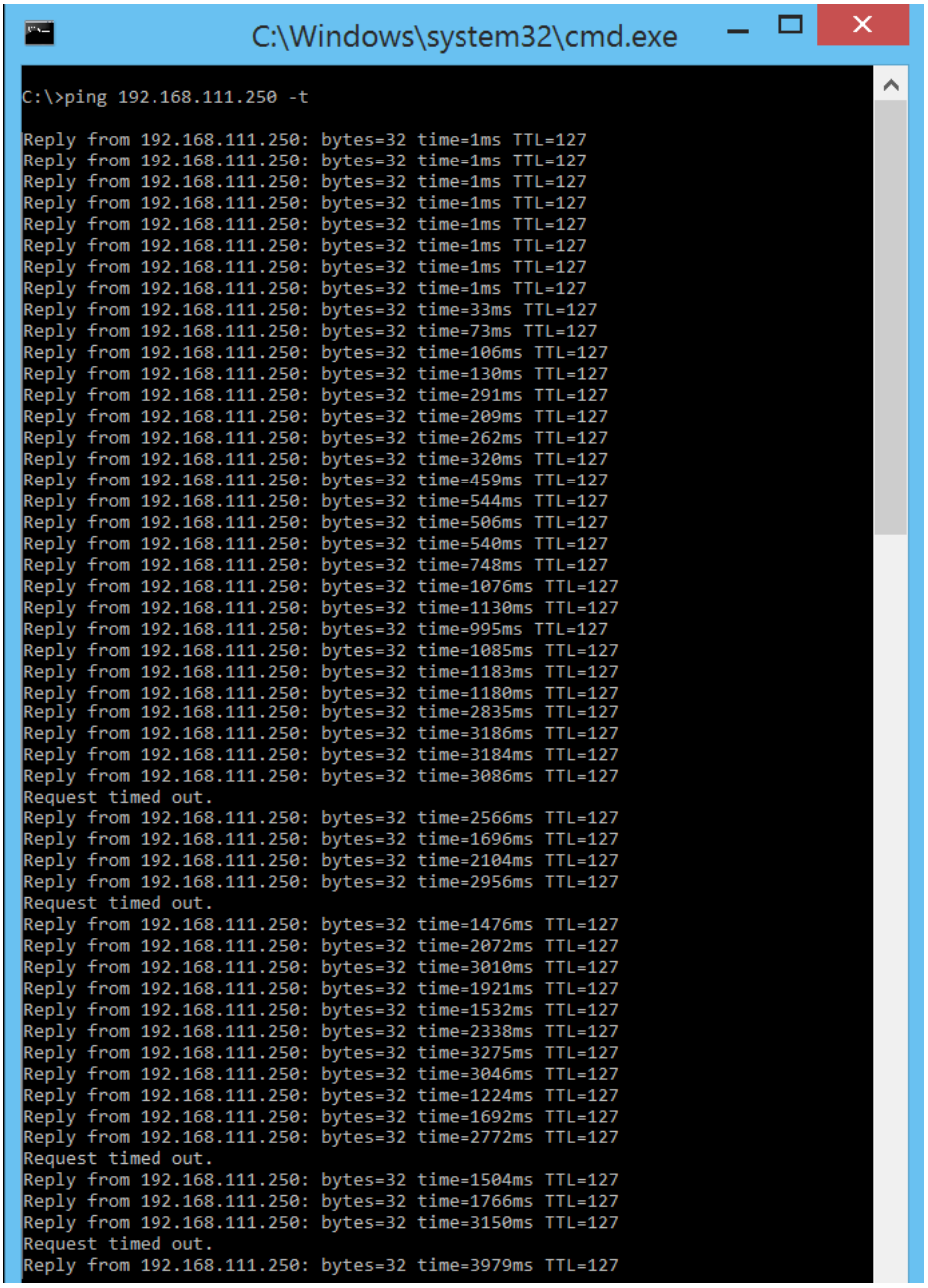
Na napadalčevem računalniku smo zagnali LOIC program. Vnesli smo ustrezen IP naslov spletnega strežnika glede na požarni zid, ki smo ga testirali. Izbrali smo napad preko TCP protokola na port 80, z 10.000 sočasnimi nitmi.



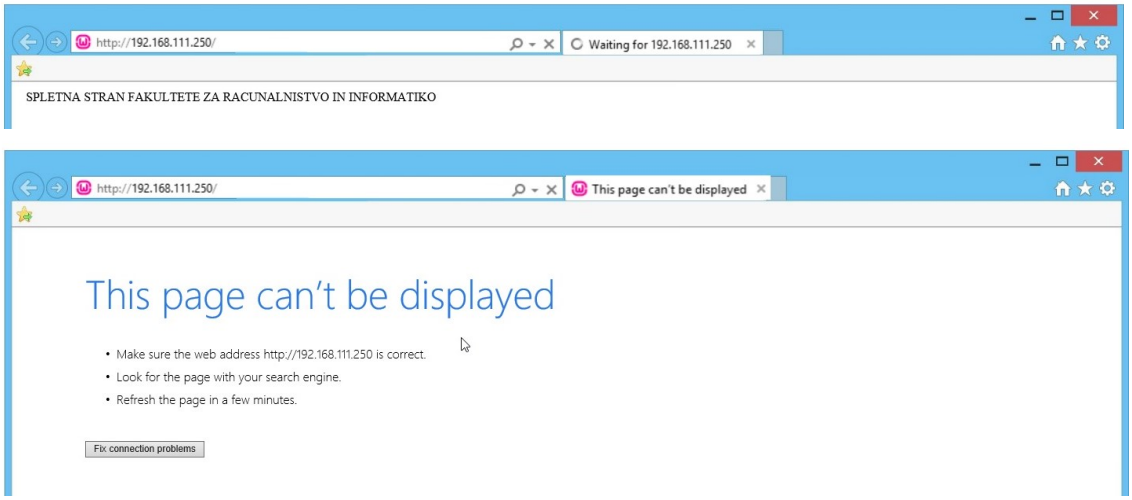
Slika 61: Konfiguracija LOIC aplikacije pri DOS napadu

4.12.3 Rezultati testov

Med samim testov smo iz kontrolnega računalnika spremljali odzivne čase spletnega strežnika, preko ukaza PING ter brskali po naši testni spletni strani. Ob zagonu DOS napada so se odzivni časi drastično povišali. Tudi brskanje po spletni strani je bilo oteženo – stran je bila večino časa nedosegljiva oz. je bil čas odgovora dolg. Na požarnem zidu smo preverili tudi količino sočasnih sej proti spletnemu strežniku.



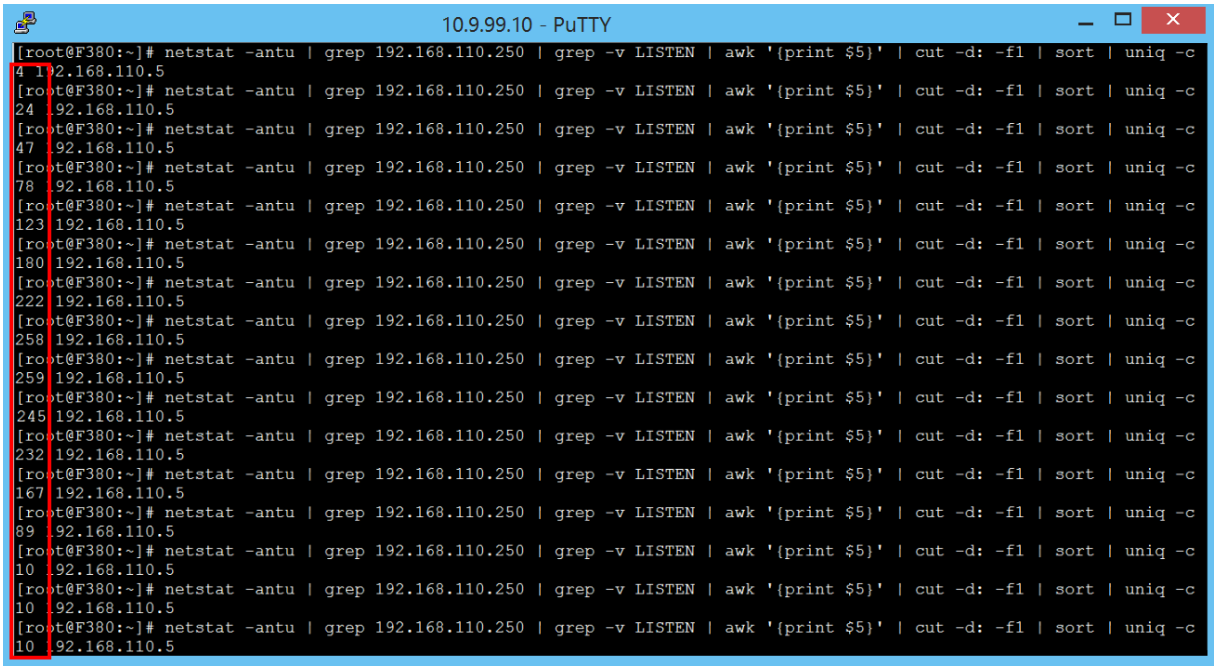
Slika 62: Prikaz odzivnih časov spletnega strežnika pred in med DOS napadom.



Slika 63: Prikaz nedosegljivosti testne spletne strani med DOS napadom.

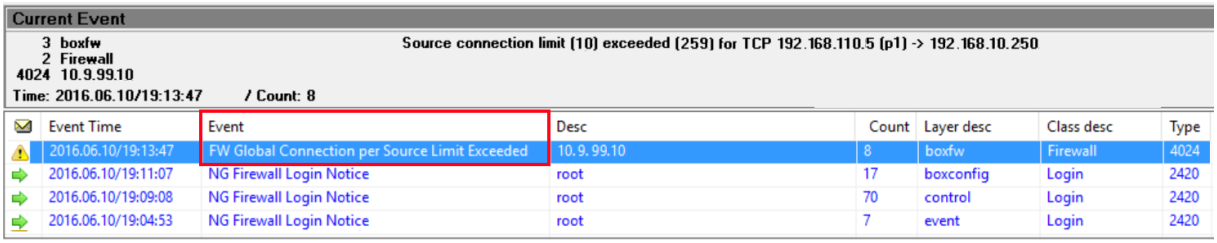
Nato smo na posameznem požarnem zidu vklopili prej pripravljena pravila za preprečevanje DOS napadov ter ponovno spremljali odzivne čase PING-a ter dosegljivost spletne strani.
Pri tem testu smo dosegli podobne rezultate pri vseh treh požarnih zidovih. Vsi požarni zidovi so uspešno omejili napadalčev računalnik na 10 sočasnih sej in tako odpravili DOS napad.

Na požarnem zidu Barracuda F380 lahko število vzpostavljenih sej med dvema IP-jema najlažje izpišemo iz CLI ukazne vrstice. Uporabimo ukaz »netstat –antu«, ki nam izpiše vse aktivne TCP in UDP povezave. Izpis nato filtriramo z ukazom »grep«, »awk« ter »cut« ter seštejemo vse pojavitve IP-ja z ukazom »uniq –c«.
Kot je razvidno iz spodnjega prikaza, je število sej pred vklopom pravila naraščalo, po vklopu pravila pa je število sej začelo počasi padati ter se ustalilo na 10.



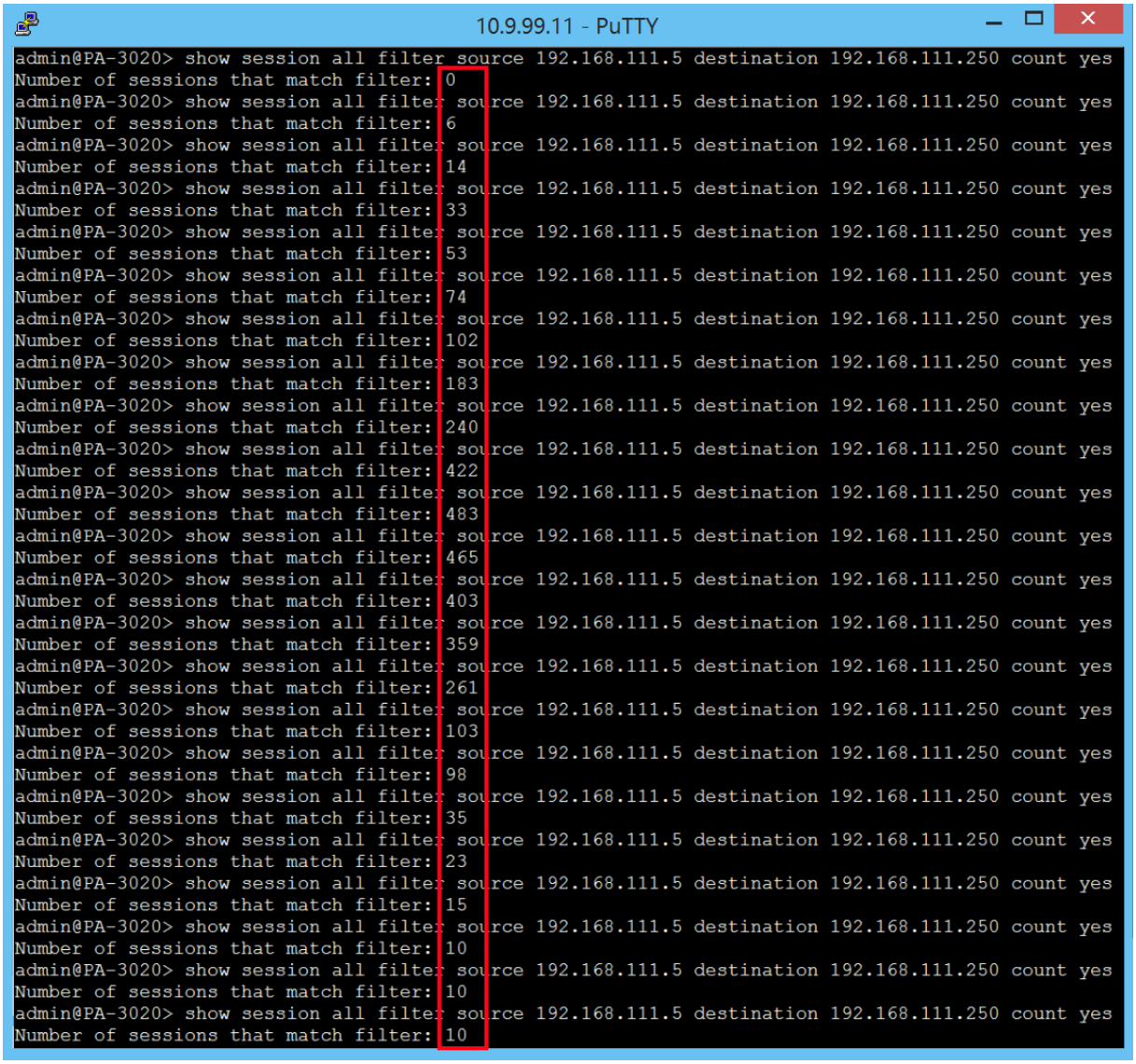
Slika 64: Prikaz izpisa števila sej na požarnem zidu Barracuda F380.

Ob proženju pravila za omejevanje števila sej požarni zid doda v dnevnik dogodkov zapis za dogodek »FW Global Connection per Source limit Exceeded« z ID številko 4024.



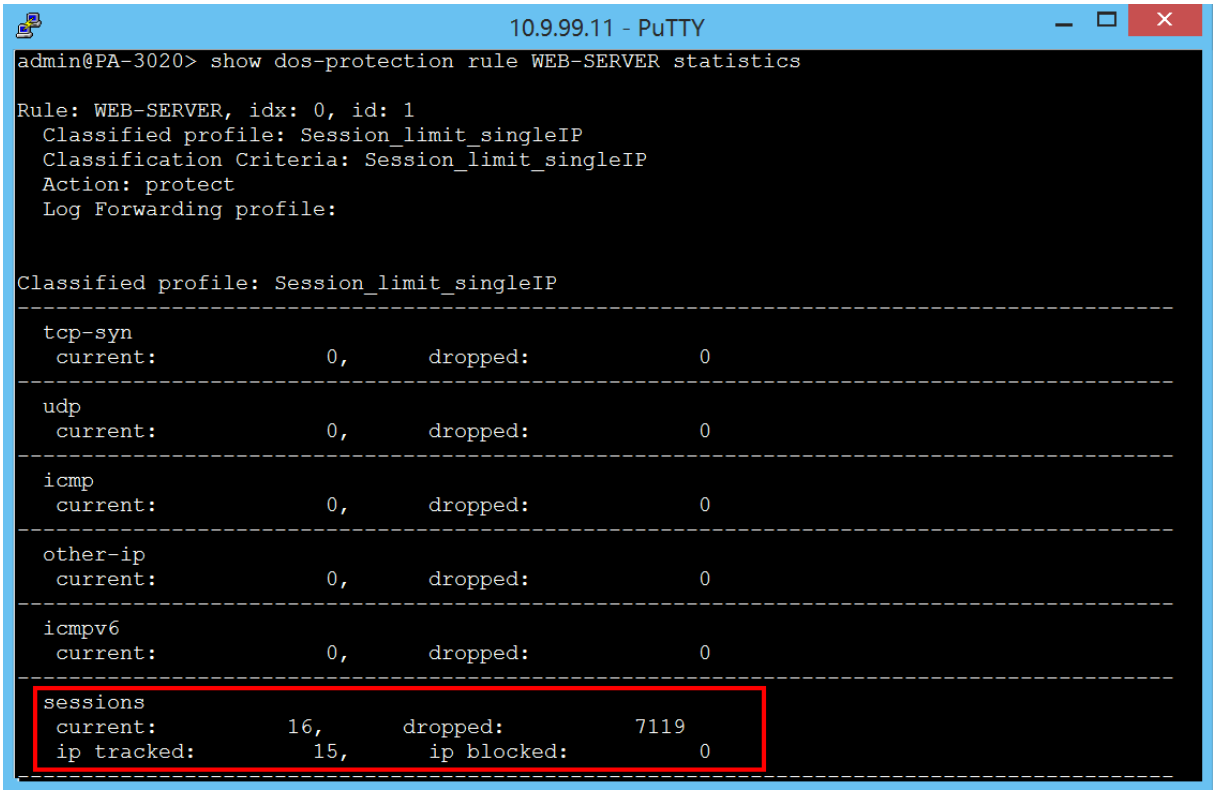
Slika 65: Prikaz zapisa v dnevniku o proženju DOS pravila na požarnem zidu Barracuda F380.

Tudi pri požarnem zidu Palo Alto PA-3020 je DOS pravilo učinkovito zmanjšalo število sočasnih sej do spletnega strežnika na 10. Število sočasnih sej med napadalcem in spletnim strežnikom smo izpisali iz CLI ukazne vrstice z ukazom »show session«. Izpis smo še filtrirali z »source« ter »destination« ukazi in jih sešteli z ukazom »count yes« tako prikazali želeni podatek.



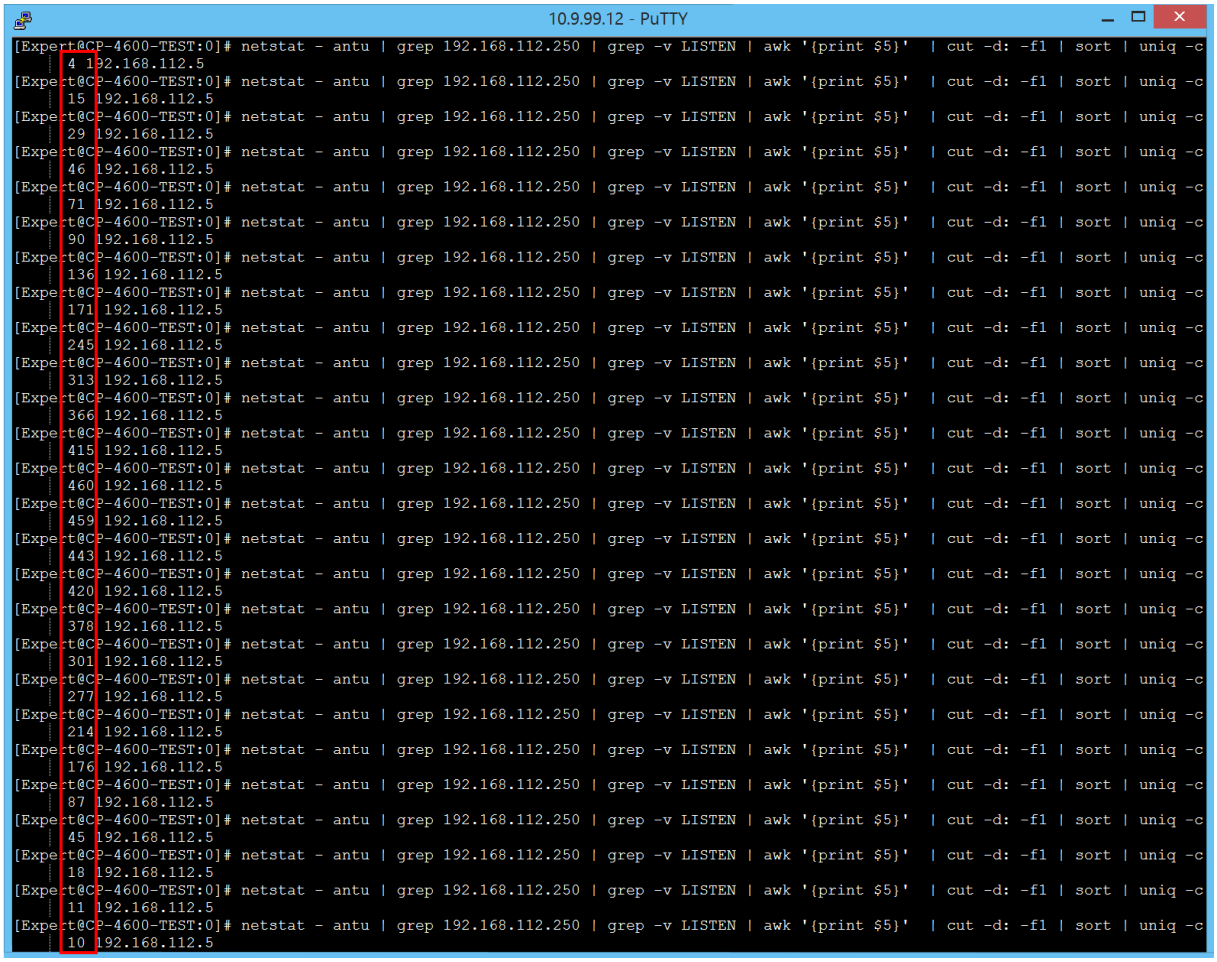
Slika 66: Prikaz izpisa števila sej na požarnem zidu Palo Alto PA-3020.

Stanje DOS pravila lahko na Palo Alto PA-3020 spremljamo iz CLI ukazne vrstice, v realnem času, z ukazom »show dos-protection rule *ime_pravila* statistics«. Požarni zid izpiše število trenutnih sej ter število ovrženih sej za posamezno pravilo.



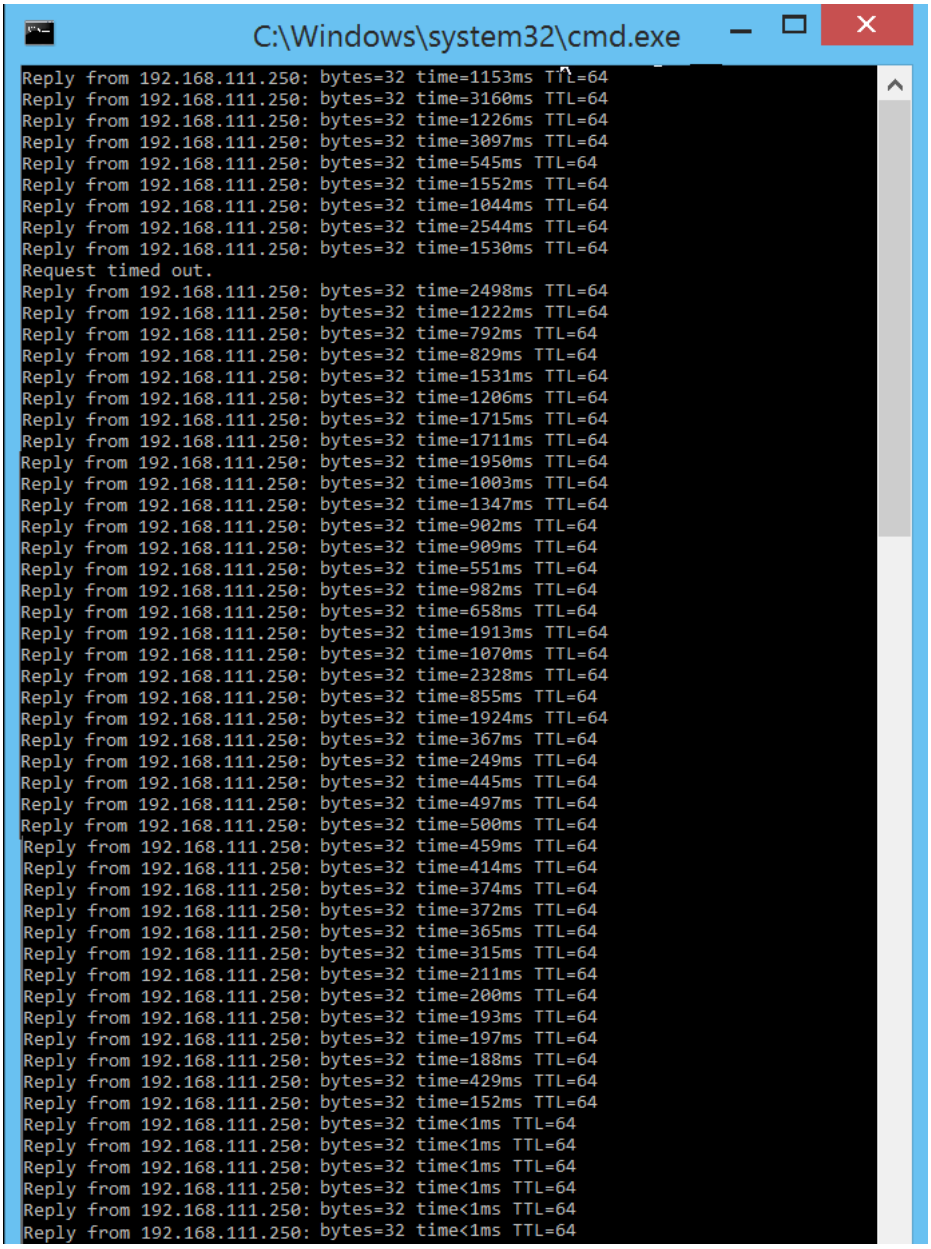
Slika 67: Izpis statistike za DOS pravilo na Palo Alto PA-3020

Podobno kot na Barracuda F380 smo tudi na Check Point 4600 izpis števila sej dosegli preko CLI ukazne vrstice z ukazom »netstat« in ustreznimi ukazi za optimizacijo izpisa.

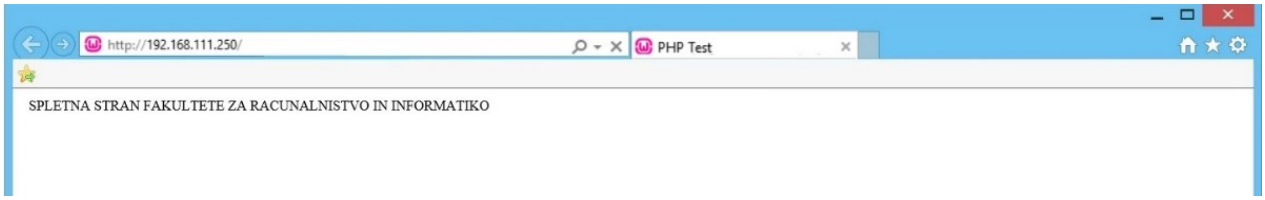


Slika 68: Prikaz izpisa števila sej na požarnem zidu Check Point 4600.

Odzivni časi spletnega strežnika so se na vseh požarnih zidovih po uvedbi DOS pravila zmanjšali, spletna stran je bila normalno dosegljiva.



Slika 69: Prikaz odzivnih časov spletnega strežnika po vklopu DOS pravila.



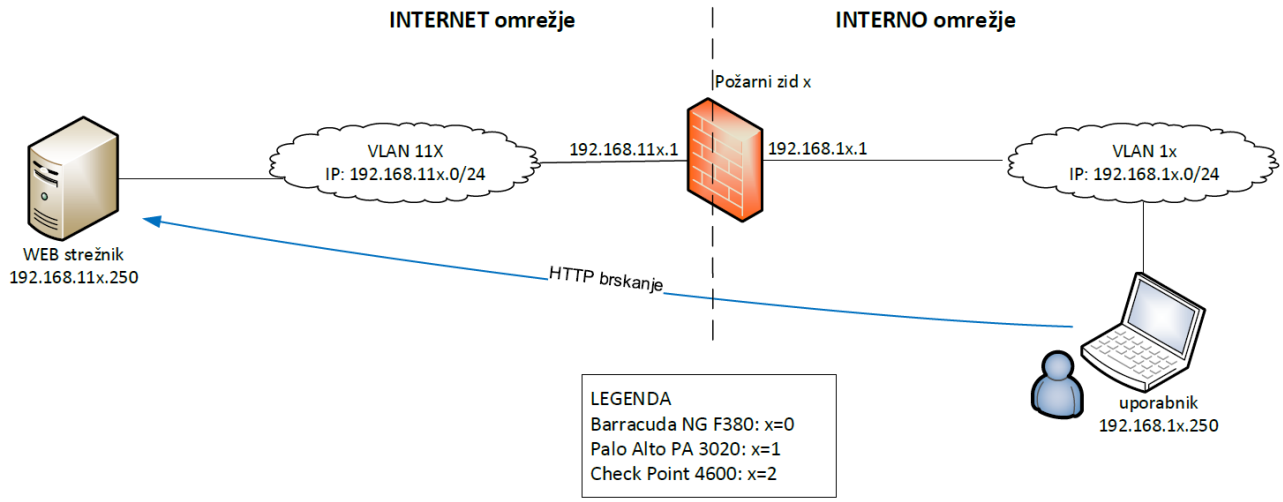
Slika 70: Prikaz testne spletne strani po vklopu DOS pravila.

4.13 Test učinkovitosti zaščite pred APT napadi

Pri testu zašite pred APT napadi so nam na pomoč priskočili inženirji iz podjetja Check Point in nam zagotovili vzorce »zero-day« groženj, s katerimi se večinoma začne APT napad. To so bili največ 7 dni stari vzorci groženj, za katere še ni bilo podpisov v bazah groženj naših testnih požarnih zidov. Pridobili smo dva tipa vzorcev, exe in pdf datoteke, z vgrajeno zlonamerno programsko kodo. Vzorce smo shranili na testni WEB strežnik ter omogočili prenos le teh iz strežnika k uporabniku, preko protokola HTTP.

Na požarnih zidovih smo poleg varnostnih pravil za zaščito pred vdori, virusi in zlonamerno programsko opremo, ki smo jih uporabili pri prejšnjem testu, nastavili še pravila za zaščito omrežja pred »zero-day« grožnjami. Vsak proizvajalec uporablja drugačno ime za omenjeno funkcionalnost, vsem pa je skupno to, da neznane vzorce datoteke pošiljajo v svoje testno okolje v oblaku, kjer se opravi analiza le teh.

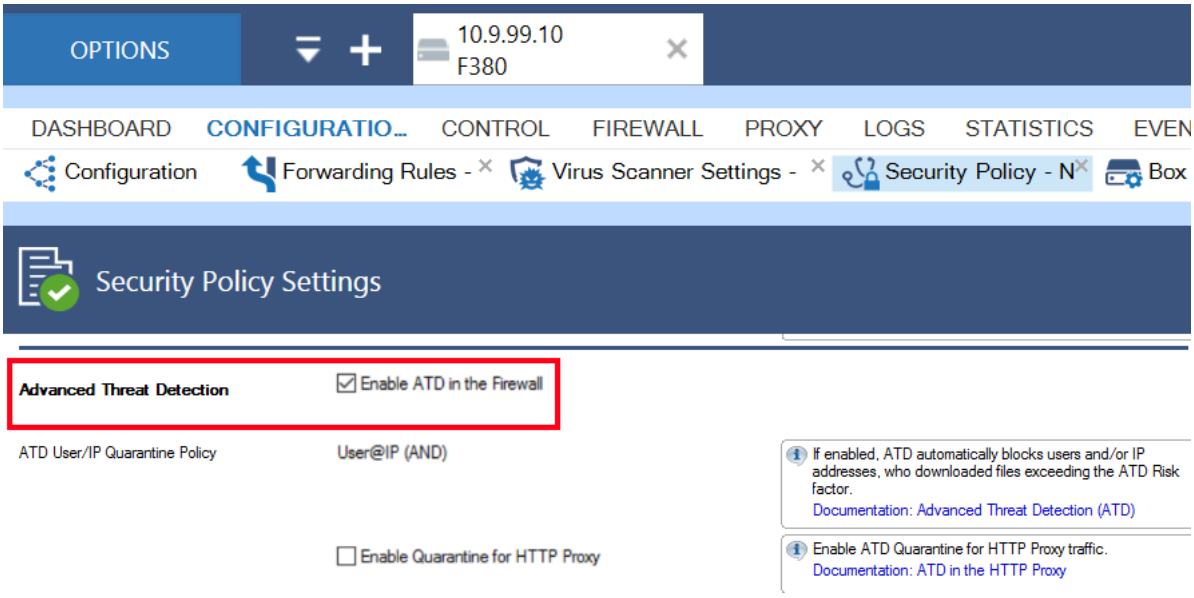
Pripravili smo še računalnik, s katerim smo simulirali uporabnika, ki prenaša datoteke iz spleta. Povezali smo se na spletni strežnik ter sprožili prenos vzorcev »Zero Day« groženj ter spremljali in beležili, koliko datotek je posamezni požarni zid zaustavil oz. posredoval v virtualno testno okolje na analizo.



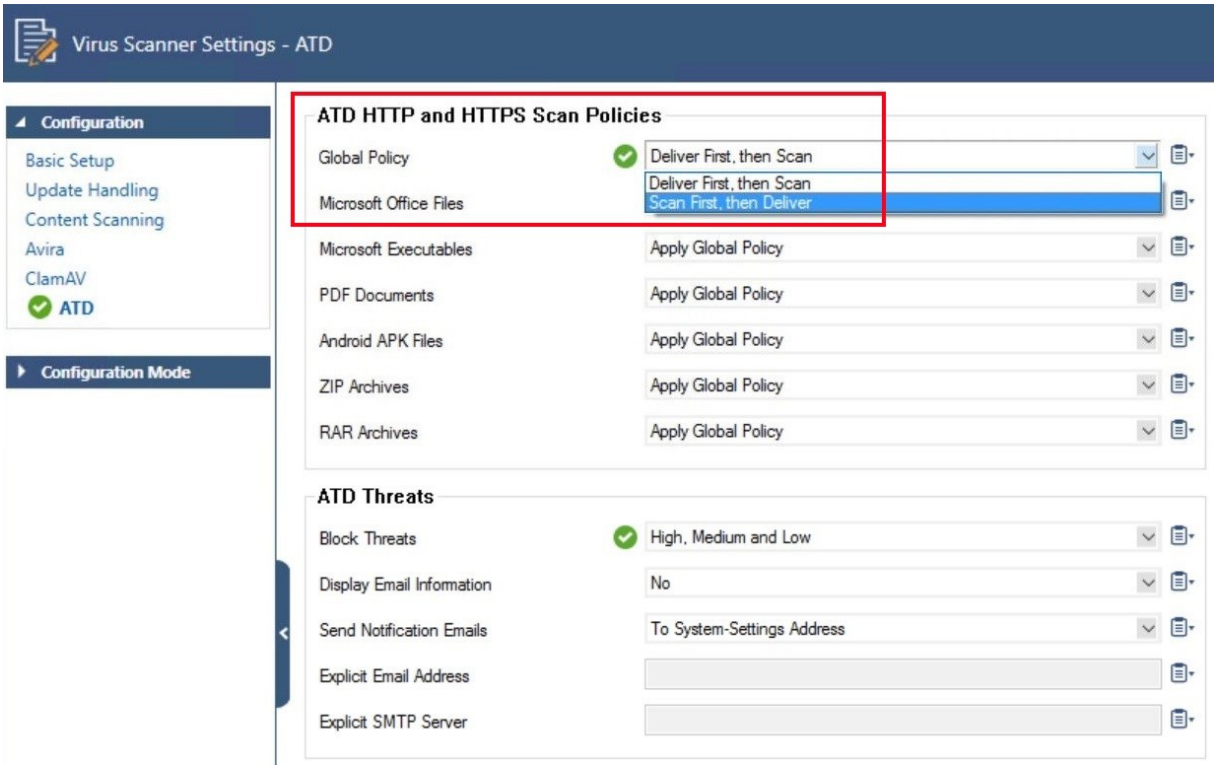
Slika 71: Shema testnega okolja pri testu zaščite pred APT napadi.

4.13.1 Konfiguracija požarnih zidov

Na požarnem zidu Barracuda F380 se tehnologija varnostne ananlize datotek v oblaku imejuje »ATD – Advanced Threat Detection«. Funkcionalnost smo najprej omogočili generalno, nato smo izbrali nastavitev, naj se neznani vzorci datoteke najprej pošlje v oblak in analizira ter v primeru, da datoteka ni okužena, posreduje uporabniku. Po skeniranju vsake datoteke v oblaku, se le tej dodeli stopnjo nevarnosti: nizka, srednja in visoka. Glede na stopnjo nevarnosti lahko nato izberemo ali naj se datoteka posreduje uporabniku ali ne. V testu smo uporabili pravilo, naj požarni zid blokira datoteke vseh treh nivojev.

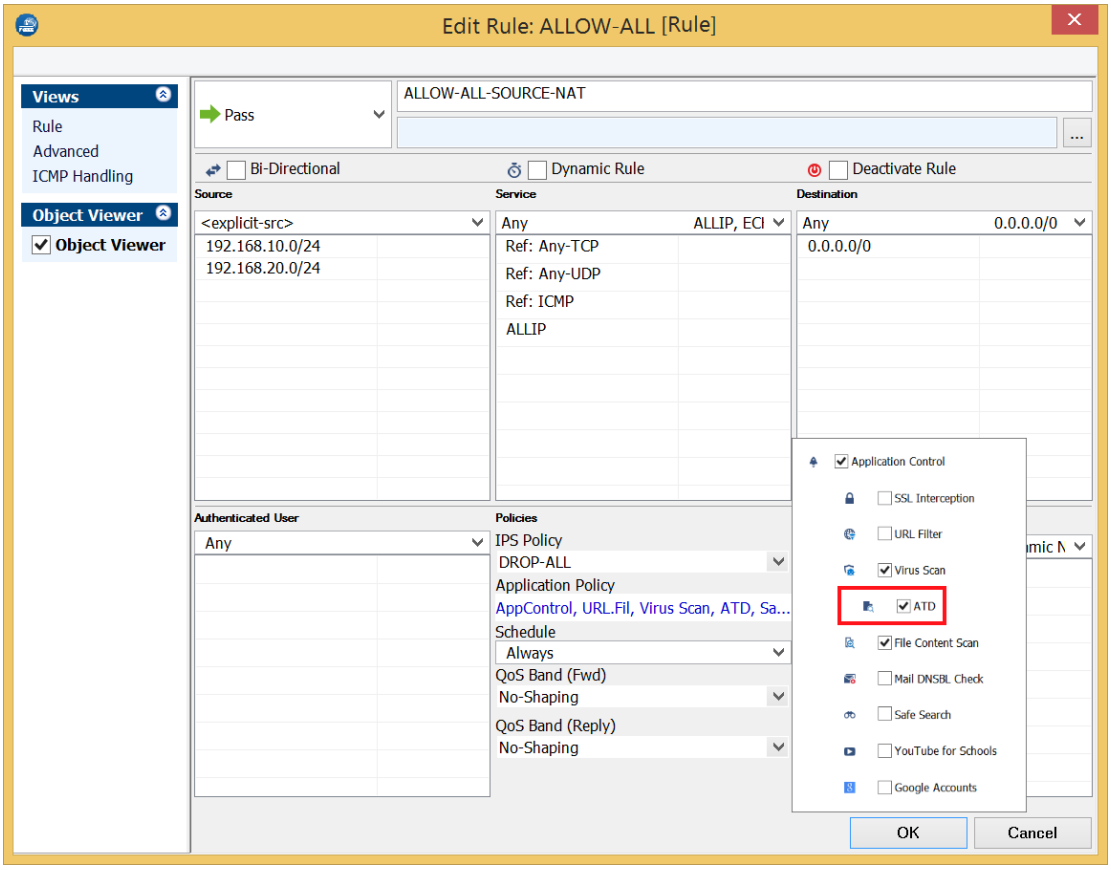


Slika 72: Prikaz vklopa ATD funkcionalnosti na požarnem zidu Barracuda F380.



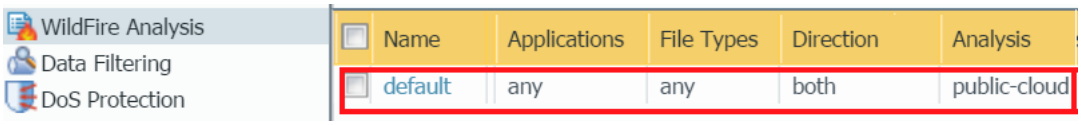
Slika 73: Prikaz izbire načina ATD posredovanja datotek na požarnem zidu Barracuda F380.

V varnostnem pravilu, ki dovoljuje dostop uporabnika iz INTERNEGA omrežja do spletnega strežnika v INTERNET omrežju, smo vključili opcijo »ATD« ter tako omogočili posredovanje neznanih datotek v oblak.



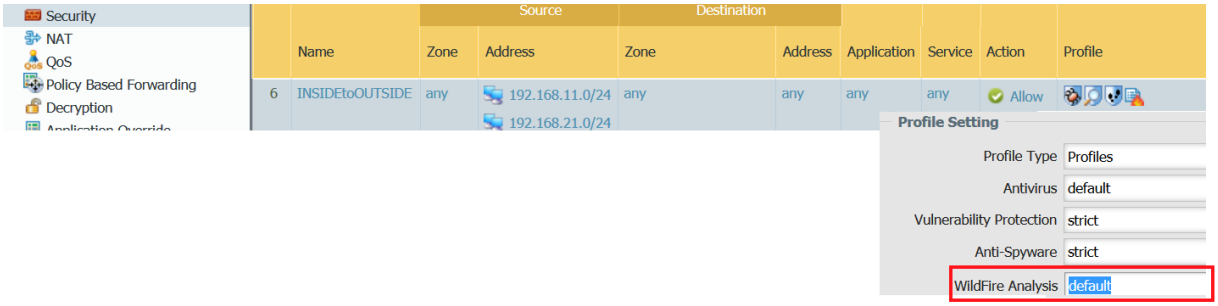
Slika 74: Varnostno pravilo z vklopom ATD funkcionalnosti na požarnem zidu Barracuda F380.

Proizvajalec Palo Alto je svojo storitev varnostne analize neznanih datotek v oblaku poimenoval »WildFire«. Pri testu smo uporabili že pripravljen »default« profil, ki v oblak pošlje vse datoteke, ne glede na tip datoteke ali smer prenosa. Palo Alto PA-3020 ne ponuja možnosti izbire načina posredovanja datotek v oblak, datoteke najprej posreduje uporabniku ter jih sočasno pošlje tudi v oblak na varnostno analizo. V kolikor se izkaže, da je datoteka okužena, o tem obvesti administratorja preko elektronske pošte.



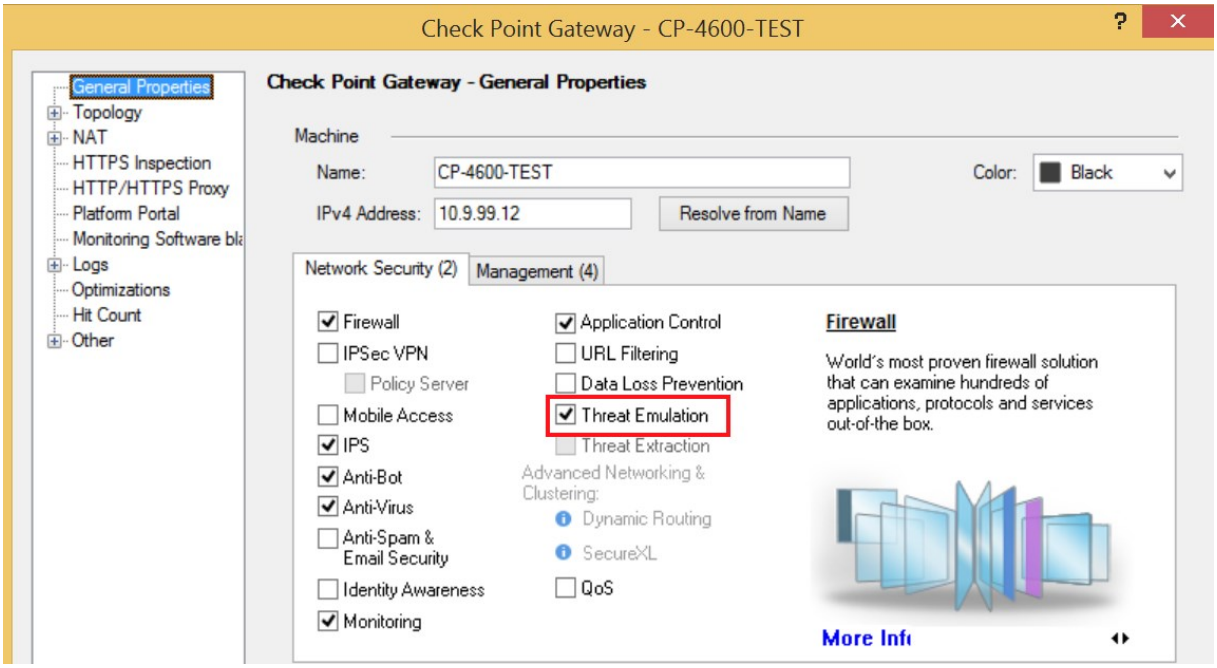
Slika 75: Priprava Wildifre profila na požarnem zidu Palo Alto PA-3020.

Wildfire profil »default« smo nato aplicirali v varnostnem pravilu, ki dovoljuje promet do testnega spletnega strežnika.



Slika 76: Apliciranje Wildifre »default« profila v varnostnem pravilu na požarnem zidu Palo Alto PA-3020,

Na požarnem zidu Check Point 4600 se tehnologija varnostne analize datotek v oblaku imejuje »Threat Emulation«. Podobno kot na požarnem zidu Barracuda F380 smo funkcionalnost najprej omogočili generalno.



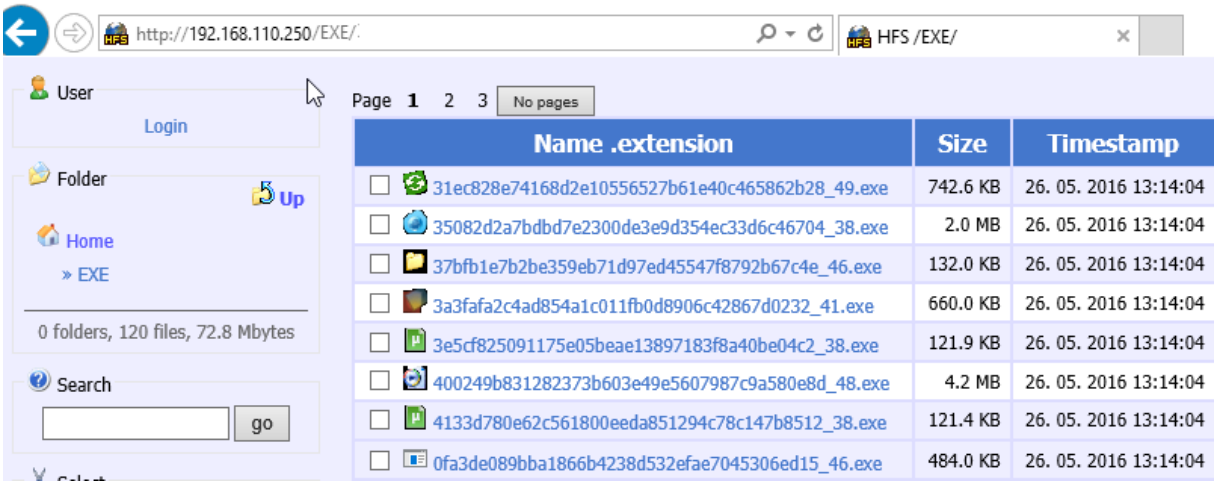
Slika 77: Prikaz vklopa »Threat Emulation« funkcionalnosti na požarnem zidu Check Point 4600.

Nato smo v pravilu za preprečevanje groženj dodali še »Threat Emulation« funkcijo. Pravilo velja za celoten promet, ki prečka požarni zid.

Slika 78: Vklop »Threat Emulation« funkcije v pravilu za preprečevanje groženj na požarnem zidu Check Point 4600.

4.13.2 Konfiguracija testerjev

V testnem okolju smo pripravili spletni strežnik in mu dodelili IP naslov iz »INTERNET« omrežja. Nanj smo namestili aplikacijo »HTTP File Server«, ki omogoča, da uporabnik prenaša datoteke iz strežnika preko brskalnika, z uporabo protokola HTTP. Vzorce »zero day« groženj smo shranili v dve mapi, glede na tip datoteke: EXE ter PDF, v vsaki je bilo po 120 vzorcev, in mape dodali v aplikacijo za prenos.



Slika 79: Prikaz spletne strani z vzorci »zero day« groženj v brskalniku.

Računalnik, s katerim smo simulirali uporabnika, ki brska po spletu, smo umestili v INTERNO omrežje. Nanj smo namestili brskalnik Mozilla Firefox, z dodatkom »Download them all«, za avtomatiziran prenos datotek iz spletnih strani ter sprožili prenos vseh 120 datotek sočasno.

4.13.3 Rezultati testov

Pri testu smo spremljali, koliko izmed 120 vzorcev groženj bo požarni zid prestregel ter koliko vzorcev izmed tistih, ki jih je uporabnik uspel prenesti preko požarnega zidu, je ta poslal v peskovnik na varnostno analizo. Rezultati so prikazani v spodnjih dveh tabelah, ločeno, glede na tip datoteke.

Število groženj predstavlja celotno število vzorcev groženj posameznega tipa, ki smo jih prenašali. Prenesene grožnje so vse datoteke, ki smo jih uspešno prenesli oz. shranili na računalnik uporabnika. Grožnje v peskovniku pa so tiste grožnje, ki jih požarni zid ni ustavil, vendar jih je zaznal kot »zero day« grožnje ter jih posredoval v oblak na varnostno analizo.

EXE datoteke			
Požarni zid	število groženj	prenesene grožnje	grožnje v peskovniku
Barracuda NG F380	120	0	0
Palo Alto PA-3020	120	104	85
Check Point 4600	120	114	110

Tabela 2: Tabela rezultatov testiranja zaščite pred APT napadi za EXE datoteke.

PDF datoteke			
Požarni zid	število groženj	prenesene grožnje	grožnje v peskovniku
Barracuda NG F380	120	3	0
Palo Alto PA-3020	120	87	51
Check Point 4600	120	101	101

Tabela 3: Tabela rezultatov testiranja zaščite pred APT napadi za PDF datoteke.

Požarni zid Barracuda je blokiral vse grožnje tipa EXE ter tudi veliko večino groženj tipa PDF, razen treh. Požarni zid je te grožnje zaznal kot virus in jih blokiral. Na spodnji sliki je prikaz iz dnevnika dogodkov požarnega zidu, kjer je razvidno, da je požarni zid datoteke razpoznal in jih zaustavil.

AID	Action	Source	Scan Type	Destination	Info	Count
(34) Virus Scan						
S-42	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Spy.Gen3)	1
S-20	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (W2000M/Dldr.Agent.CG.405)	5
S-15	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (EXP/Pidief.cum)	6
S-26	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (EXP/CVE-2015-1770.A)	2
S-41	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Dldr.Small.uqnm)	2
S-40	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Diofopi.E.2)	1
S-39	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/ATRAPS.Gen2)	1
S-33	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (W2000M/Dldr.Agent.14901)	2
S-19	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (EXP/CVE-2012-1856.46556)	2
S-38	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (ADWARE/Agent.41472)	1
S-37	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Crypt.ZPACK.87577)	1
S-36	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (BDS/Backdoor.Gen3)	1
S-35	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (X2000M/Dldr.Agent.0600139)	1
S-32	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Crypt.ZPACK.gmfr)	1
S-34	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (W2000M/Dldr.Agent.57787)	1
S-29	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Crypt.EPACK.Gen2)	2
S-31	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Skeeyah.uulm)	1
S-30	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Skeeyah.oqnk)	1
S-28	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (EXP/Pidief.ald)	1
S-24	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Crypt.XPACK.Gen)	1
S-25	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Dropper.Gen)	2
S-22	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Agent.18432.272)	1
S-23	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Proxy.Slaper.fp.1)	1
S-21	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (W32/Agent.EA)	1
S-18	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Dldr.Agent.wqj.2)	1
S-16	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (EXP/Flash.EB.563)	1
S-17	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (EXP/FLASH.Pubenush.N.Gen)	1
S-12	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (W2000M/Dldr.Agent.14901)	1
S-11	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (W2000M/Dldr.Agent.85222222)	1
S-10	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/Crypt.EPACK.Gen2)	1
S-8	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (EXP/Pidief.cum)	3
S-9	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (W32/Agent.EA)	1
S-6	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (PUA/LoadMoney.Gen7)	2
S-7	Scan	192.168.10.250	Virus Scan	192.168.110.250	Virus Blocked (TR/ATRAPS.Gen)	2

Slika 80: Prikaz izpisov iz dnevnika dogodkov pri prenosu testnih datotek na požarnem zidu Barracuda F380.

Požarni zid Palo Alto PA-3020 je dovoli prenos večine vzorcev: 104 EXE datotek ter 87 PDF datotek. Izmed teh je na varnostno analizo v peskovnik poslal 85 oz. 51 vzorcev, kjer so bili vsi opredeljeni kot zlonamerni. Vzorce, ki jih je blokiral, je razpoznal kot virus. Požarni zid je vsak blokiran oz. analiziran vzorec ter rezultat analize zapisal v dnevnik dogodkov, kar je prikazano na spodnjih slikah.

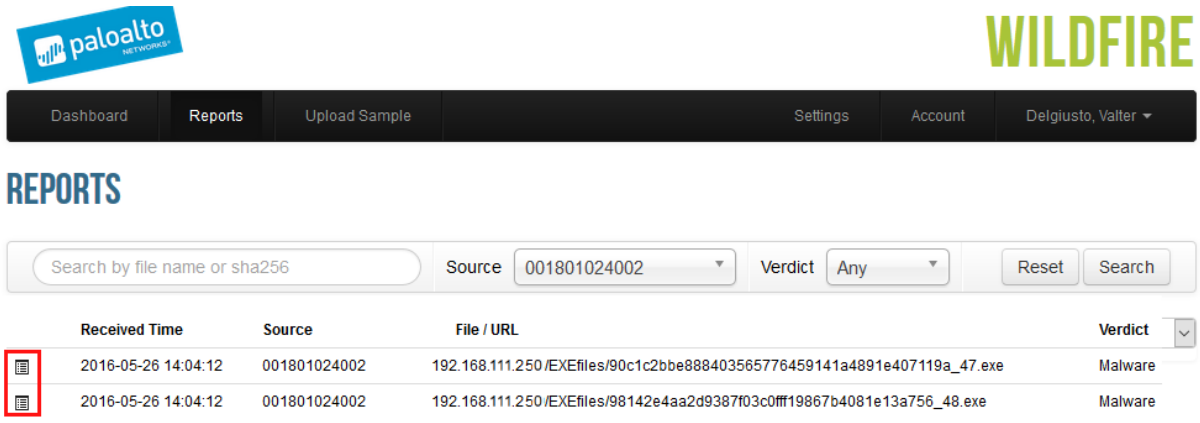
Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity	Severity
wildfire-virus	Trojan/Win32.sakurel.d	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60640	web-browsing	reset-both	medium	medium
wildfire-virus	Virus/Win32.WGeneric.jbrxp	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60629	web-browsing	reset-both	medium	medium
wildfire-virus	Trojan/Win32.sakurel.d	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60626	web-browsing	reset-both	medium	medium
wildfire-virus	Virus/Win32.WGeneric.jbjbz	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60625	web-browsing	reset-both	medium	medium
wildfire-virus	Virus/Win32.WGeneric.jbrxp	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60624	web-browsing	reset-both	medium	medium
wildfire-virus	Trojan/Win32.sakurel.d	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60612	web-browsing	reset-both	medium	medium
wildfire-virus	Virus/Win32.WGeneric.jbrxp	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60617	web-browsing	reset-both	medium	medium
wildfire-virus	Trojan/Win32.sakurel.d	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60611	web-browsing	reset-both	medium	medium
wildfire-virus	Virus/Win32.WGeneric.jbjbz	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60606	web-browsing	reset-both	medium	medium
wildfire-virus	Virus/Win32.WGeneric.jbrxp	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	60605	web-browsing	reset-both	medium	medium

Slika 81: Prikaz izpisov iz dnevnika dogodkov za datoteke zaznane kot virus na požarnem zidu Palo Alto PA-3020.

File Name	Source Zone	Destination Zone	Attacker	Victim	Desti... Port	Application	Verdict
eb13062dfc8a17c56fd5fc40cecd3c40a504daa3_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62162	web-browsing	malicious
aaf8387752cbbddddcc386b161c80ec70833b922_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62129	web-browsing	malicious
aaf8387752cbbddddcc386b161c80ec70833b922_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62133	web-browsing	malicious
59a8c88c0aed3b042485466317108aec7f42a85c_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62089	web-browsing	malicious
59a8c88c0aed3b042485466317108aec7f42a85c_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62092	web-browsing	malicious
27fe14c456bf11eb891e26ae9be25941393f0dfd_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62086	web-browsing	malicious
27fe14c456bf11eb891e26ae9be25941393f0dfd_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62089	web-browsing	malicious
0d05bf2450ef7157dc9ec4a59dd592907a74299d_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62054	web-browsing	malicious
0d05bf2450ef7157dc9ec4a59dd592907a74299d_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62056	web-browsing	malicious
27fe14c456bf11eb891e26ae9be25941393f0dfd_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62291	web-browsing	malicious
aaf8387752cbbddddcc386b161c80ec70833b922_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62247	web-browsing	malicious
59a8c88c0aed3b042485466317108aec7f42a85c_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62207	web-browsing	malicious
59a8c88c0aed3b042485466317108aec7f42a85c_34.pdf	OUTSIDE	INSIDE	192.168.111.250	192.168.11.250	62205	web-browsing	malicious

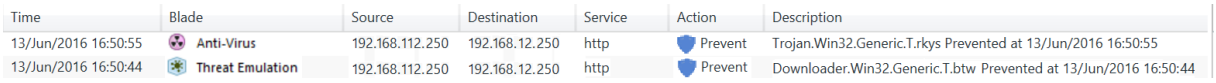
Slika 82: Prikaz izpisov iz dnevnika dogodkov za datoteke analizirane v oblaku na požarnem zidu Palo Alto PA-3020.

Palo Alto nudi možnost spletne prijave v storitev »WildFire«, kjer lahko pridobimo več podatkov o datotekah, ki so bile analizirane v oblaku. Za vsako izmed teh lahko prenesemo poročilo v PDF obliki, z natančnimi podatki o zlonamerni kodi v datoteki ter testnem okolju, kjer je bila testirana.



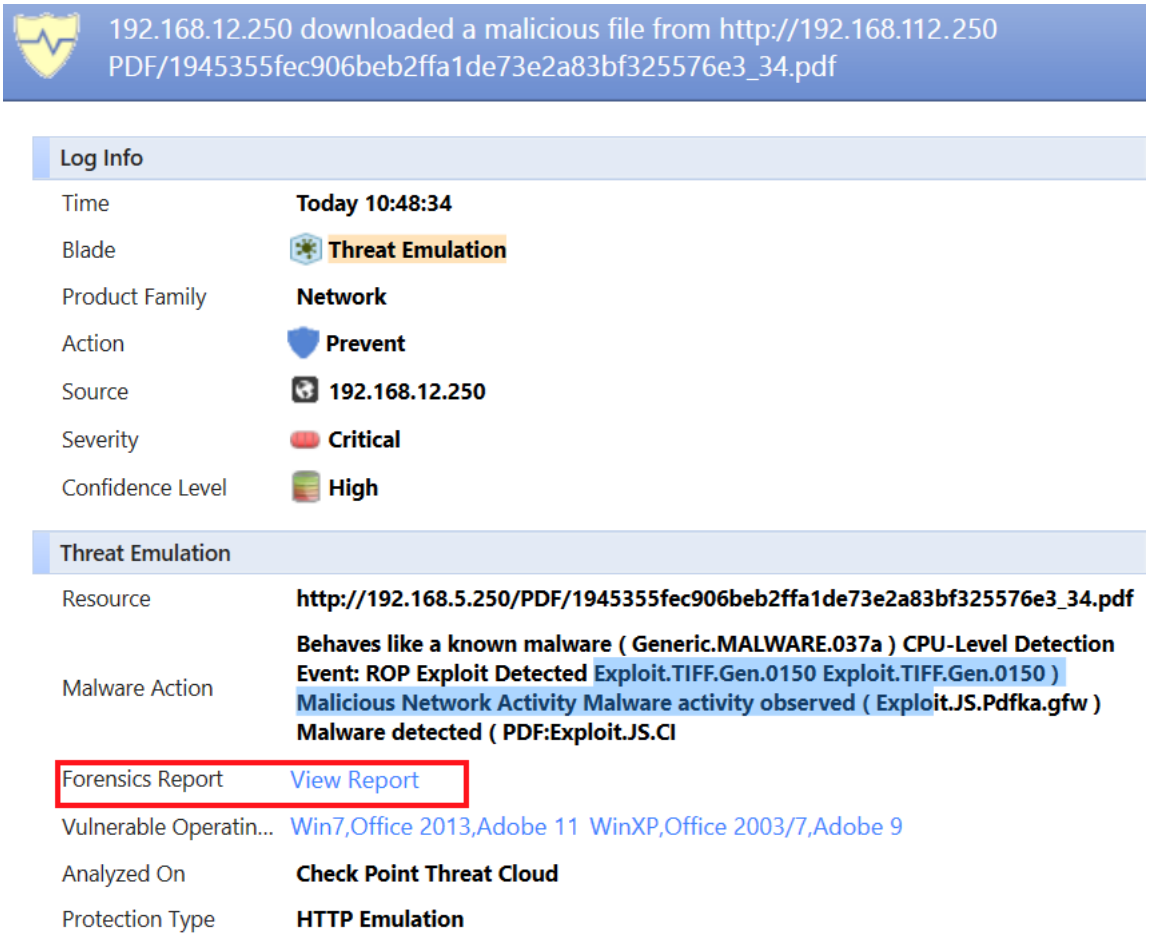
Slika 83: Prikaz spletne storitve »WildFire« z možnostjo ogleda poročila o varnostni analizi.

Preko požarnega zidu CP smo uspeli prenesti 114 EXE ter 101 PDF datotek. Od tega je požarni zid CP poslal na varnostno analizo v oblak 110 EXE ter vse PDF datoteke. Blokirane datoteke je razpoznal kot virus ter to zapisal v dnevnik dogodkov pod dogodek tipa »Anti-Virus. Pod tip dogodka »Threat Emulation« pa je zapisal posredovanje datotek v oblak. Oba zapisa sta prikazana na spodnji sliki.



Slika 84: Prikaz izpisov iz dnevnika dogodkov pri testu zaščite pred APT napadi na požarnem zidu CP.

Ob kliku na dogodek »Threat Emulation« se odpre pojavno okno, z natančnejšimi podatki o samem dogodku. S klikom na povezavo »View Report« pa si lahko ogledamo obširno poročilo o varnostni analize obravnavane datoteke v oblaku, ki vsebuje podatke o vsebovani zlonamerni kodi (kako se koda obnaša, katere procese je zagnala in katere registre je spremenila na računalnikih v testnem okolju) ter podatke o samem testnem okolju.



Slika 85: Prikaz pojavnega okna za dogodek »Threat Emulation« na požarnem zidu CP.

5. Analiza ter interpretacija rezultatov

5.1 Testi prepustnosti

Pri testih prepustnosti smo na vseh treh požarnih zidovih dosegli pričakovane rezultate ali celo boljše od pričakovanih.
Pri testu požarnega zidu Barracuda F380 smo na vseh testih dosegli vsaj takšno prepustnost, kot jo navaja proizvajalec v tehnični dokumentaciji oz. specifikacijah naprave. Pri testih prepustnosti, z vklopljeno funkcionalnostjo za preprečevanje groženj, je ta celo presegla podatke iz specifikacije. Pri testu ostalih dveh požarnih zidov, pa smo dosegli prepustnosti enake nazivnim.
Pri tem velja omeniti, da je funkcionalnost preprečevanja groženj tista, ki je za požarni zid najbolj obremenjujoča. Požarni zid mora ves promet podrobno analizirati ter ga primerjati z bazo definicij groženj. Večja kot je baza definicij, več časa potrebuje požarni zid, da določi, ali promet morebiti vsebuje škodljivo programsko opremo. Baza definicij groženj na požarnem zidu Barracuda F380 obsega trenutno 3.675 zapisov, v bazah ostalih dveh požarnih zidov pa je okoli 9.000 zapisov. Ta podatek torej predstavlja enega izmed morebitnih vzrokov za razlike v prepustnosti med požarnimi zidovi.

5.2 Test zaščite pred DOS napadi

Vsi trije požarni zidovi so svojo nalogo pri zaznavi in odpravi DoS napada opravili brez težav. Pred vklopom pravila za DoS zaščito je pri vseh treh požarnih zidovih prišlo do podobnih težav: visoki odzivni časi spletnega strežnika, spletna stran je zelo slabo odzivna, oziroma je bila večino časa nedosegljiva, število sej iz napadalčeva IP naslova se je nenehno povečevalo. Pravilo za DoS zaščito je na vseh treh požarnih zidovih delovalo brezhibno in v kratkem času zmanjšalo število sej na samo deset. Požarni zidovi so nas o morebitnem poteku DoS napada tudi obvestili, saj smo lahko opazili zapise o proženju DoS pravila v dnevnikih zapisov požarnih zidov. Sočasno so se zmanjševali tudi odzivni časi spletnega strežnika in spletna stran je bila ponovno normalno dosegljiva.
Ker so vrste in metode DoS napadov znane in dokaj statične, predstavljajo požarni zidovi naslednje generacije učinkovito zaščito pred napadi te vrste. S pravilno konfiguracijo in doslednostjo, lahko spletne strežnike učinkovito obvarujemo. Ker pa se zaščita pred DoS napadi začne že veliko preden promet doseže naš požarni zid, je pri DoS zaščiti še posebej pomembno sodelovanje internet ponudnikov pri blokiranju takšnega prometa, preden doseže naš požarni zid.

5.3 Test zaščite pred APT napadi

Pri testu zaščite pred APT napadi so nas rezultati presenetili. Pričakovali smo, da bosta požarna zidova Palo Alto PA-3020 in Check Point 4600, ki sta dražja in tudi dalj časa prisotna na trgu, dosegla bolšje rezultate kot Barracuda F380, ki je na trg požarnih zidov naslednje generacije vstopil pred kratkim. Rezultati testov pa kažejo obratno sliko. Protivirusni sistem požarnega zidu Barracuda F380, ki uporablja bazo definicij virusov znanega protivirusnega programa Avira, je zaznal in blokiral veliko večino groženj. Potrebe po pošiljanju neznanih datotek v peskovnik ni bilo.
Požarni zid Palo Alto PA-3020 nam je sicer dovolil prenesti okoli 75 odstotkov datotek, tri četrtine teh pa je posredoval v peskovnik na analizo, kjer jih je nato označil kot zlonamerno kodo. Na računalnik uporabnika smo torej uspeli prenesti 55 od 240 okuženih datotek.
Tudi požarni zid Check Point 4600 je dovolil prenos velike večine datotek, vendar je tudi skoraj vse zaznal kot »zero-day« grožnje in jih prenesel v svoje okolje, za analizo »SandBlast«. Rezultati analize so datoteke označili za škodljive.
Na tem mestu velja še enkrat omeniti, da so bili uporabljeni vzorci zlonamerne programske opreme ustvarjeni iz strani proizvajalca Check Point.

Za uspešno izvedbo testiranj smo morali nastaviti najprej osnovne parametre požarnih zidov, ter jih nato z vsakim nadaljnjim testov nadgrajevati, z vse bolj kompleksnimi konfiguracijami. Požarna zidova Palo Alto in Check Point nudita po našem mnenju bolj pregleden in intuitiven uporabniški vmesnik kot Barracuda, pri katerem je za vklop nekaterih funkcionalnosti potrebna sprememba na več neodvisnih sklopih konfiguracije. Palo Alto ima še to prednost, da lahko vse nastavitve požarnega zidu od prvega koraka dalje opravimo iz enotnega vmesnika – bodisi spletnega vmesnika bodisi CLI ukazne vrstice.

Pri testih prepustnosti nas je požarni zid Barracuda prijetno presenetil. Ker gre za manj znan in relativno nov produkt v segmentu požarnih zidov naslednje generacije, smo pričakovali slabše rezultate kot pri že uveljavljenih požarnih zidovih, kot sta Palo Alto in Check Point. Zadnja dva sta se pri testih prepustnosti sicer odrezala korektno. Zmogljivosti, ki jih proizvajalca navajata v dokumentaciji in opisu produktov, so realne. Požarni zid Barracuda pa je uradno navedeno zmogljivost celo presegel.

Rezultati testov zaščite pred DoS napadi so bili pričakovani. Izvedli smo volumetrični DoS napad, za katerega so tehnike preprečevanja znane. Vsi trije požarni zidovi na testu imajo vdelane mehanizme za njihovo preprečevanje in so jih brez težav ustavili. Zanimivo bi bilo

izvesti tudi teste aplikacijskega DoS napada, katerega preprečevanje zahteva analizo prometa na aplikacijskem TCP/IP sloju. Za izvedbo takšnega testa bi potrebovali zelo drago in napredno opremo oziroma botnet , ki pa ju žal nismo imeli na razpolago.

Najzanimivejši pa so bili testi zaščite pred naprednimi grožnjami, pri katerih nismo vedeli, kaj pričakovati. Zero-day grožnje, ki smo jih imeli na razpolago, so napisali strokovnjaki za omrežno varnost. Bile naj bi enakovredne grožnjam, ki jih uporabljajo dejanski napadalci, pri vsakodnevnih napadih na omrežja. Spet nas je presenetil požarni zid Barracuda F380, ki je uspel zaustaviti skoraj vse grožnje. Tudi požarni zid Check Point 4600 je uspešno prepoznal večino groženj in upravičil sloves enega izmed vodilnih proizvajalcev v segmentu požarnih zidov naslednje generacije. Drugi vodilni proizvajalec v tem segmentu - Palo Alto, pa je pri tem testu dosegel najslabše rezultate izmed treh požarnih zidov. Možen vzrok je lahko ta, da je vzorce groženj napisal proizvajalec, ki je neposreden konkurent.
Vsi trije požarni zidovi so se izkazali kot učinkovite rešitve za zaščito in so presegli naša pričakovanja.

6. Zaključek

Informacijske tehnologije in internet, kot ključni element le teh, se bodo v prihodnje vsekakor nenehno širile in razvijale. Trendi poslovanja neizogibno vodijo v popolno digitalizacijo vseh delovnih procesov, kar s seboj prinese drastično večanje količine informacij in občutljivih podatkov v digitalni obliki. Večina teh podatkov se tudi pretaka po svetovnem spletu. Tudi v privatnem življenju informacije večinoma shranjujemo v elektronski obliki. Naj gre za fotografijo, položnico ali pismo, le še redko jih srečujemo v klasični obliki. Informacije v digitalni obliki so za moderno civilizacijo vse bolj ključnega pomena.
Zaradi tega lahko pričakujemo še večji porast kibernetskega kriminala, kateremu pridobitev osebnih, bančnih in nasploh vseh občutljivih podatkov lahko prinese ogromne dobičke. Zato morajo organizacije, ki hranijo takšne vrste podatkov, narediti vse, da bi to preprečile. Informacijska varnost mora slediti hitremu tempu razvoja novih tehnologij in nuditi orodja za učinkovito zašito le teh.
Požarni zidovi so eden izmed ključnih elementov pri ohranjanju varnosti. Postavljeni so v »prvo bojno linijo«, saj ločujejo varovana omrežja od nevarovanih. Tradicionalni požarni zidovi že nekaj časa niso doživeli korenitih sprememb in niso sposobni slediti tehničnemu napredku, zato je bil prihod naprednejših in »pametnejših« naprav nujen.

V diplomskem delu smo hoteli raziskati ali so požarni zidovi naslednje generacije sposobni zadostiti današnjim potrebam po visokih hitrostih povezovanja in ali pripomorejo k ustrezni zaščiti vse bolj ogroženih sodobnih omrežij.

Testi prepustnosti so pokazali, da so požarni zidovi naslednje generacije tudi, kar se tiče prepustnosti, naredili velik korak naprej, v primerjavi s klasičnimi požarnimi zidovi. Pri testih vseh treh produktov smo dosegli visoke hitrosti povezovanja, ki zagotovo zadostijo potrebam velike večine organizacij. Hitrosti povezovanja okoli 1Gbps se danes uporabljajo predvsem v internem omrežju, v smeri interneta so v uporabi hitrosti do nekaj sto Mbps. Požarni zidovi naslednje generacije so po zmogljivostih povezovanja torej primerni za umestitev v sodobna omrežja organizacij, saj presegajo zmogljivosti, ki jih te trenutno potrebujejo. Zato bodo, kljub konstantnemu nadgrajevanju pasovne širine, tudi v prihodnjih nekaj letih zadovoljili potrebe po visokih hitrostih povezovanja v internet.
Bistvene razlike in izboljšave pa so požarni zidovi naslednje generacije prinesli pri preprečevanju sodobnih groženj. Testi preprečevanja DoS napadov so pokazali, da moderni požarni zidovi brezhibno opravljajo nalogo zaščite prek takšnimi napadi. Požarni zidovi imajo tehnologijo in mehanizme, ki znajo preprečiti večino modernih DoS napadov.

Žal pa lahko organizacija utrpi škodo zaradi DoS napada, kljub temu, da njen požarni zid svojo nalogo opravi 100 odstotno. Pri DoS napadu je namreč požarni zid, nameščen neposredno pred strežnik, zadnji člen v verigi preprečevanja le tega. V kolikor ponudniki internet storitev nimajo ustrezne opreme in znanja za zaznavo in blokiranje takšnega prometa, lahko napadalec zasede celotno pasovno širino operaterja in tako onemogoči komunikacijo do celotne organizacije, ne samo določenega strežnika. Žal je zaradi vse večje konkurence na trgu ponudnikov storitev in želje, po čim večjih zaslužkih, vlaganje ponudnikov internet storitev v tovrstno zaščito majhno. Tako so organizacije primorane za DoS zaščito poskrbeti same.

Svojo pravo dodano vrednost pa so požarni zidovi naslednje generacije pokazali pri testih preprečevanja APT napadov. Uspešno so zaznali in blokirali večino »*Zero-day*« groženj in na ta način preprečili vstop škodljive programske opreme v omrežje.
Požarni zidovi naslednje generacije po našem mnenju niso samo primerno, ampak nujno orodje v sodobni informacijski varnosti. Nudijo inovativen vpogled v omrežni promet in veliko naprednih funkcionalnosti, brez katerih zagotavljanje varnosti v prihodnje ne bo več mogoče. Seveda pa požarni zid sam po sebi ni dovolj za zaščito in mora biti smiselno vključen v celovit varnostni sistem organizacij. Vodilni kader, administratorji in zaposleni se morajo zavedati pomena varnosti in dobrih praks ter biti dobro poučeni. Noben sistem ni popolnoma zaščiten pred vdori. Napadalec, s pravo kombinacijo znanja, potrpežljivosti, motivacije in sredstev, bo prej ali slej vdrl v vsak sistem, ki meji na zunanje omrežje. V sodobni resničnosti informacijske varnosti se mora organizacija odločiti, kateri podatki so zanjo najbolj pomembni in sprejeti dodatne ukrepe za njihovo zaščito ob vdoru v sistem.

7. Literatura

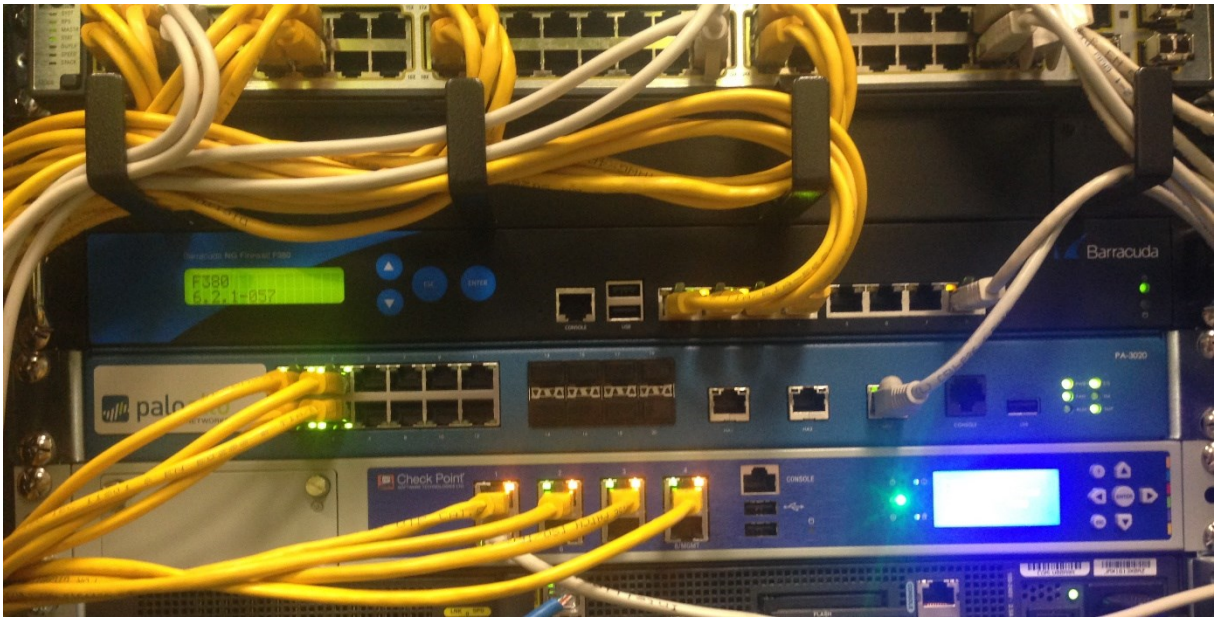
[1] Kurt Thurber (2013) Past and Present Security Threats: A Decade of Malware Evolution. Dostopno na:
http://blog.productcentral.aol.com/2013/08/08/past-and-present-security-threats/
[2] (2015) Kaspersky. Dostopno na:
https://usa.kaspersky.com/internet-security-center/threats/top-7-cyberthreats#.V3_IDaJq1S1
[3] (2009) CARNet. Dostopno na:
http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-09-240.pdf
[4] (2015) WikiIS. Dostopno na:
http://www.cis.hr/WikiIS/doku.php?id=dos_attacks
[5] Wei Wei, Feng Chen, Yingjie Xia, Guang Jin (2013) A Rank Correlation Based Detection against Distributed Reflection DoS Attacks. Dostopno na:
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6400346&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6400346
[6] Matthew Prince (2016) Technical Details Behind a 400Gbps NTP Amplification DDoS Attack. Dostopno na:
https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/
[7] Marek Majkowski (2016) 400Gbps: Winter of Whopping Weekend DDoS Attacks. Dostopno na:
https://blog.cloudflare.com/a-winter-of-400gbps-weekend-ddos-attacks/
[8] Colin Tankard (2011) Advanced Persistent threats and how to monitor and deter them. Dostopno na:
http://www.sciencedirect.com/science/article/pii/S1353485811700861
[9] Daša Janja Banovec (2014) Napredne trajne grožnje in usmerjen kibernetski napad na organizacije. Dostopno na:
http://www.fvv.um.si/dv2014/zbornik/Banovec.pdf
[10] (2011) Symantec. Dostopno na:
http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf
[11] (2012) Help Net Security. Dostopno na:
https://www.helpnetsecurity.com/2012/12/05/how-the-eurograbber-attack-stole-36-million-euros/
[12] Margaret Rouse (2015) Firewall. Dostopno na:
http://searchsecurity.techtarget.com/definition/firewall
[13] (2016) Studytonight. Dostopno na:
http://www.studytonight.com/computer-networks/tcp-ip-reference-model

[14] (2005) Microsoft. Dostopno na:
https://technet.microsoft.com/en-us/library/cc786900(v=ws.10).aspx
[15] (2016) Wikipedia: Dostopno na:
https://en.wikipedia.org/wiki/Network_address_translation
[16] (2016) Symantec. Dostopno na:
https://support.symantec.com/en_US/article.HOWTO55098.html
[17] Sean Wilkins (2014) A Guide to Choosing a Next-Generation Firewall. Dostopno na:
http://www.tomsitpro.com/articles/next-generation-firewall-vendors,2-847.html
[18] John Pescatore, Greg Young (2009) Defining the Next-Generation Firewall. Dostopno na:
https://www.lan1.com.au/images/file/Brochure/Gartner-DefiningNextGenFirewalls.pdf
[19] (2016) Cymbel. Dostopno na:
https://www.cymbel.com/zero-trust-recommendations/sandbox-threat-detection/
[20] (2016) Barracuda. Dostopno na:
https://www.barracuda.com/assets/docs/Datasheets/Barracuda_NG_Firewall_DS_US.pdf
[21] (2016) PaloAlto. Dostopno na:
https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-3000-series
[22] (2016) CheckPoint. Dostopno na:
https://www.checkpoint.com/products/4000-appliances/
[23] Carolyn Mathas (2005) Agilent's N2X multiservices test is key to IPv6 readiness. Dostopno na:
http://www.eetimes.com/document.asp?doc_id=1242649
[24] Rickard Nobel (2011). Actual throughput on Gigabit Ethernet. Dostopno na:
http://rickardnobel.se/actual-throughput-on-gigabit-ethernet/
[25] (2016) Wikipedia. Dostopno na:
https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon

Dodatek A

Slika A1: Komunikacijska omarica s testno opremo

Slika A2: Generatorja omrežnega prometa Agilent Technologies N4190B



Slika A3: požarni zidovi na testu

Slika A4: požarni zidovi na testu

Slika A5: požarni zidovi na testu

Slika A6: Testni laboratorij v podjetju S&T

Kazalo slik

Kazalo tabel

Kazalo grafikonov